

Cisco DCNM Media Controller Configuration Guide, Release 11.3(1)

First Published: 2019-12-20

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

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.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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)

© 2019 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Overview** 1

Cisco Data Center Network Manager 1

REST API Tool 2

CHAPTER 2 **Dashboard** 7

Dashboard 7

Dashlets 8

CHAPTER 3 **Inventory** 13

Viewing Inventory Information 13

Viewing Inventory Information for Switches 13

Viewing System Information 17

Interfaces 18

VLAN 21

FEX 23

VDCs 26

Viewing Inventory Information for Modules 33

Viewing Inventory Information for Licenses 34

Discovery 35

Adding, Editing, Re-Discovering, Purging and Removing LAN, LAN Tasks and Switch 35

Adding LAN Switches 35

Editing LAN Devices 36

Removing LAN Devices from Cisco DCNM 37

Rediscover LAN Task 37

CHAPTER 4 **Monitor** 39

Monitoring Switch 39
Viewing Switch CPU Information 39
Viewing Switch Memory Information 39
Viewing Switch Traffic and Errors Information 40
Viewing Switch Temperature 40
Enabling Temperature Monitoring 41
Viewing Accounting Information 41
Viewing Events Information 42
Monitoring LAN 42
Monitoring Performance Information for Ethernet 42
Monitoring ISL Traffic and Errors 43
Monitoring a vPC 44
Monitoring vPC Performance 45
Alarms 46
Viewing Alarms and Events 47
Monitoring and Adding Alarm Policies 47
Activating Policies 50
Deactivating Policies 50
Importing Policies 50
Exporting Policies 51
Editing Policies 51
Deleting Policies 51
Enabling External Alarms 51
Health Monitor Alarms 52

CHAPTER 5 **Configure** 55
Deploy 55
POAP Launchpad 55
Power-On Auto Provisioning (POAP) 55
DHCP Scopes 56
Image and Configuration Servers 58
POAP Templates 60
POAP Template Annotation 62
POAP Definitions 64

Cable Plan 70
Templates 72
Template Library 72
Template Library 72
Configuring Jobs 101
Backup 102
Switch Configuration 102
Copy Configuration 103
View Configuration 104
Delete Configuration 104
Compare Configuration Files 104
Export Configuration 105
Import Configuration File 106
Restore Configuration 106
Archive Jobs 107
Archives 110
Compare Configuration Files 111
View Configuration 112
Network Config Audit 112
Generating Network Config Audit Reports 112
Image Management 114
Upgrade [ISSU] 114
Upgrade History [ISSU] 114
Switch Level History 121
Patch [SMU] 121
Installation History 122
Switch Installed Patches 124
Package [RPM] 125
Package Installation [RPM] 125
Switch Installed Packages 128
Maintenance Mode [GIR] 128
Maintenance Mode 128
Switch Maintenance History 129
Image and Configuration Servers 130

Add Image or Configuration Server URL 130
Deleting an Image 131
Editing an Image or Configuration Server URL 131
File Browser 131
Image Upload 132
LAN Telemetry Health 132
Health 133
Software Telemetry 133
Flow Telemetry 140

CHAPTER 6 **Media Controller** 147
Topology 149
Host 150
Discovered Host 150
Host Alias 151
Add Host Alias 152
Edit Host Alias 152
Delete Host Alias 153
Import Host Alias 153
Export Host Alias 153
Host Policies 154
Add Host Policy 159
Edit Host Policy 160
Delete Host Policy 160
Import Host Policy 161
Export Host Policy 161
Policy Deployment 162
Applied Host Polices 163
Flow 164
Flow Status 164
Flow Alias 168
Add Flow Alias 169
Edit Flow Alias 169
Delete Flow Alias 170

Export Flow Alias 170
Import Flow Alias 170
Flow Policies 171
Add Flow Policy 176
Edit Flow Policy 176
Delete Flow Policy 177
Import Flow Policy 177
Export Flow Policy 178
Policy Deployment 178
RTP 180
RTP Flow Monitor 180
Global 184
Events 184
Config 185
Setting Up the SNMP Server for DCNM 185
AMQP Notifications 185
Switch Global Config 187
WAN Links 190
DCNM Read-Only Mode for Media Controller 193

CHAPTER 7 **Administration** 199
DCNM Server 199
Starting, Restarting, and Stopping Services 199
Customization 200
Viewing Log Information 201
Server Properties 202
Configuring SFTP/TFTP/SCP Credentials 202
Modular Device Support 205
Managing Switch Groups 206
Adding Switch Groups 206
Removing a Group or a Member of a Group 207
Moving a Switch to Another Group 208
Native HA 208
Multi Site Manager 210

Manage Licensing 210
Managing Licenses 210
License Assignments 211
Server License Files 216
Switch Features—Bulk Install 217
Management Users 219
Remote AAA 219
Local 220
Radius 220
TACACS+ 221
Switch 221
LDAP 221
Managing Local Users 224
Adding Local Users 224
Deleting Local Users 224
Editing a User 225
User Access 225
Managing Clients 226
Performance Setup 226
Performance Setup LAN Collections 227
Performance Setup Thresholds 227
Event Setup 228
Viewing Events Registration 228
Notification Forwarding 229
Adding Notification Forwarding 229
Removing Notification Forwarding 231
Event Suppression 231
Add Event Suppression Rules 231
Delete Event Suppression Rule 232
Modify Event Suppression Rule 232
Credentials Management 233
LAN Credentials 233
Credentials Management with Remote Access 235

CHAPTER 8 **Applications** 241

Cisco DCNM in Unclustered Mode 241

Cisco DCNM in Clustered Mode 242

Requirements for Cisco DCNM Clustered Mode 242

Installing a Cisco DCNM Compute 244

Networking Policies for OVA Installation 244

Enabling the Compute Cluster 246

Managing Application Network Pools 247

Adding Computes into the Cluster Mode 248

Transitioning Compute Nodes 250

Transitioning Compute nodes from VM to Service Engine 250

Transitioning Compute nodes from Service Engine to VM 251

Preferences 251

Telemetry Network and NTP Requirements 252

Installing and Deploying Applications 253

Application Framework User Interface 256

Catalog 257

Health Monitor 258

Alerts 258

Service Utilization 260

Compute Utilization 263

PTP Monitoring 263

Compute 265

Preferences 267

Failure Scenario 267

Compute Node Disaster Recovery 268

CHAPTER 9 **DCNM Integration with ServiceNow** 269

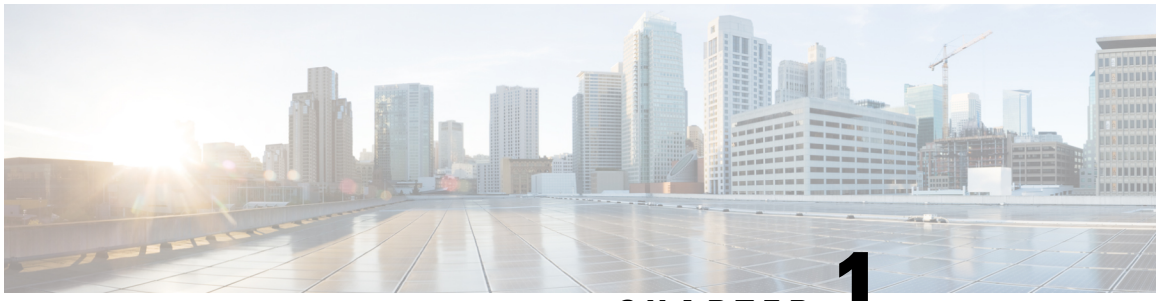
DCNM Integration with ServiceNow 269

Guidelines and Limitations of DCNM Integration with ServiceNow 270

Installing and Configuring the Cisco DCNM Application on ServiceNow 270

Viewing the Dashboard 273

Troubleshooting DCNM Integration with ServiceNow 275



CHAPTER 1

Overview

- Cisco Data Center Network Manager, on page 1
- REST API Tool, on page 2

Cisco Data Center Network Manager

Cisco Data Center Network Manager (Cisco DCNM) automates the infrastructure of Cisco Nexus 5000, 6000, 7000, and 9000 Series Switches and Cisco MDS 9000 Series switches. Cisco DCNM enables you to manage multiple devices, while providing ready-to-use capabilities, such as, control, automation, monitoring, visualization, and troubleshooting.

Note The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

The Cisco DCNM home page contains a navigation pane to the left, and shortcuts to a few Cisco DCNM features in the middle pane.

This guide provides comprehensive information about the UI functionality for Cisco DCNM Media Controller deployment.

The top pane displays the following UI elements:

- **Help**: Launches the context-sensitive online help.
- *User Role*: Displays the role of the user who is currently logged in, for example, admin.
- **Gear** icon: Click on the gear icon to see a drop-down list with the following options:
  - **Logged in as**: displays the user role of the current logged in user.
  - **Change Password**: Allows you to change the password for current logged in user.

    If you are a **network administrator** user, you can modify the passwords of the other users.
  - **About**: Displays the Version, Installation Type, and time since when the Web UI is operational.

- **REST API Tool**: Allows you to examine the APIs invoked for every operation. See the *REST API Tool* section for more information about the API inspection.
- **Logout**: Allows you to terminate the Web UI and returns to the login screen.

For more information about Cisco DCNM, see:

https://www.cisco.com/c/en/us/support/cloud-systems-management/data-center-network-manager-11/model.html.

REST API Tool

Operations like discovery, fabric management, monitoring, and so on, which are performed in Cisco DCNM Web UI, invoke HTTP calls to fetch and commit the information accessed. The REST API tool enables you to examine the API call by viewing the structure of an API call. This tool also provides a corresponding CURL request to help with building quick prototypes and testing APIs.

The **REST API Tool** dialog box has the following fields.

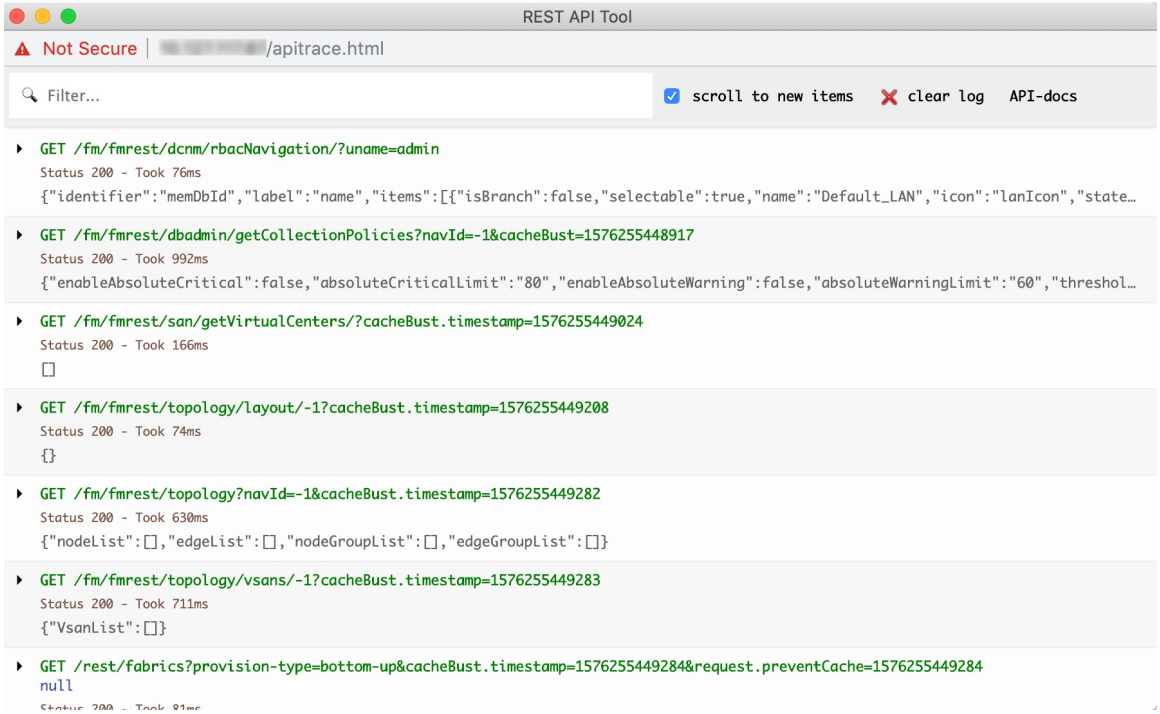
Table 1: Fields and Description for the REST API Tool Dialog Box

Field	Description
Filter	Enter any keyword to search the log.
scroll to new items	Check this check box to scroll to the new entries when you navigate back to the **REST API Tool** dialog box after you perform an operation in the Web UI. This check box is checked by default.
clear log	Click **clear log** to clear the log in the dialog box.
API-docs	Click API-docs to view the Cisco DCNM REST API documentation in the Web UI. Clicking this option takes you to the following URL: https://*DCNM-IP*/api-docs

All actions you perform in the Cisco DCNM Web UI appear in the API inspector tool. The following information appears in the APIs invoked for every operation:

- HTTP method
- URI
- Payload
- HTTP status code
- Time taken for the operation

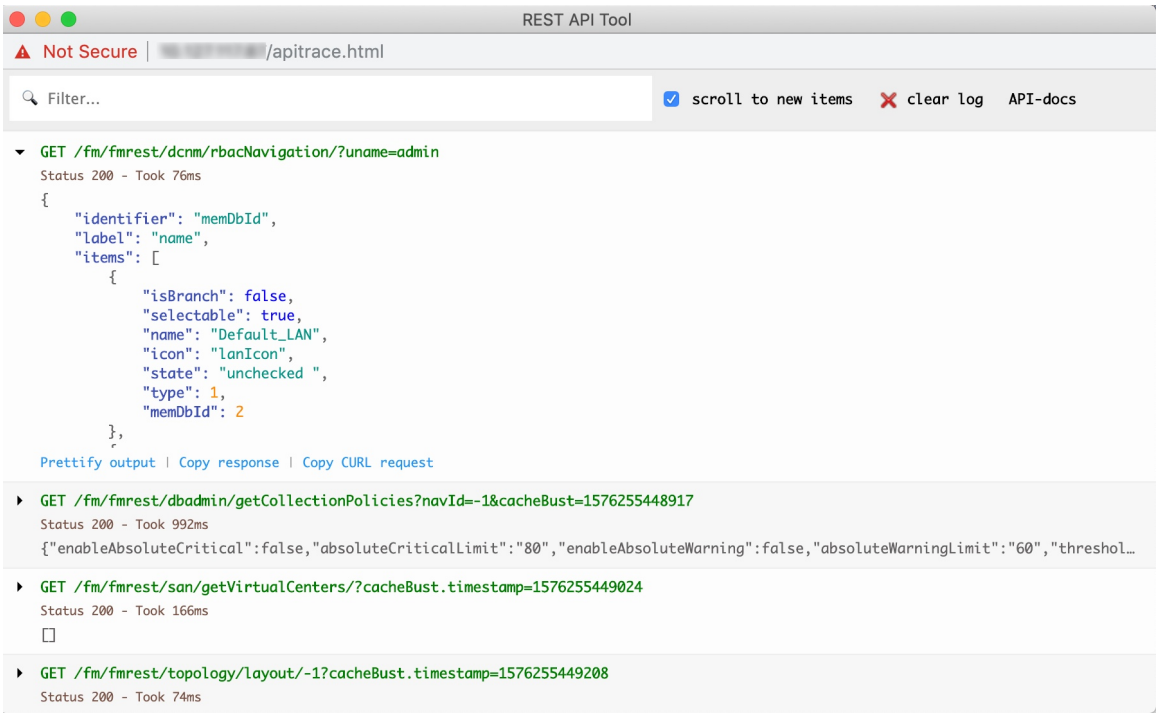
The following image displays how the log appears in the **REST API Tool** dialog box.



Click the URI to expand or collapse each REST method. You can perform the following actions after expanding a REST method:

- **Prettify output**: Click this option to arrange the response code in a more presentable way, which otherwise appears in a single line. Scroll through the response to view it completely.
- **Copy response**: Click this option to copy the response code to your clipboard.
- **Copy CURL request**: Click this option to copy the CURL request to your clipboard.

```
curl -k -XGET --header 'Dcnm-Token: <DCNM_TOKEN>' --header 'Content-Type:
application/x-www-form-urlencoded'
https://<ip-address>/fm/fmrest/dcnm/rbacNavigation/?uname=admin
```



The **REST API Tool** dialog box updates every time the Cisco DCNM Web UI updates.

To use the API inspector from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Click the **Gear** icon in the top pane.

Step 2 Choose **REST API Tool** from the drop-down list.

The **REST API Tool** dialog box appears and the log is empty before you perform any operation in the Cisco DCNM Web UI.

Step 3 Minimize the **REST API Tool** dialog box.

Note You can also keep the dialog box open, but not close it.

Step 4 Perform an operation in the Cisco DCNM Web UI.

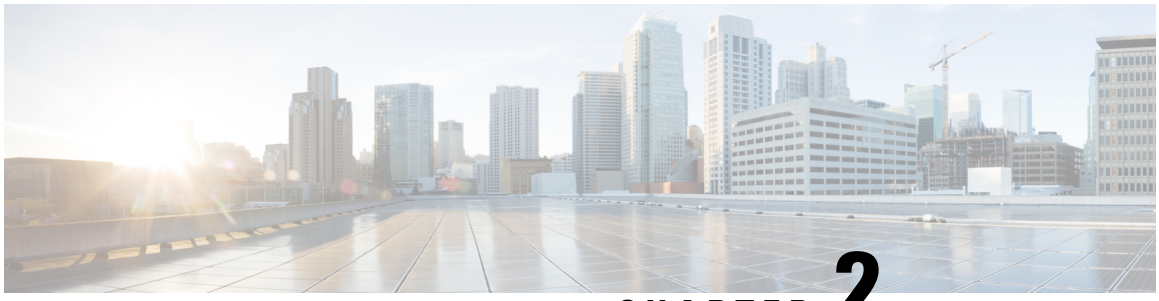
Note You can perform any operation in the Cisco DCNM Web UI like viewing any options, adding, deleting, and so on.

Step 5 Navigate back to the **REST API Tool** dialog box.

The log is populated with the REST APIs fetched depending on the operations you performed.

Note Closing the **REST API Tool** dialog box, instead of minimizing it before performing any operations, clears the log.

For a demo on some of the operations that can be performed using the REST API tool, see the Using REST API Tool in Cisco DCNM video.



CHAPTER 2

Dashboard

This chapter contains the following topics:

- Dashboard, on page 7

Dashboard

The intent of **Dashboard** is to enable network and storage administrators to focus on particular areas of concern around the health and performance of data center switching. This information is provided as 24-hour snapshots. The functional view of LAN switching consists of six dynamic dashlets that display information in the context of the selected scope by default. The scope can be adjusted in the upper right corner of the window to display focused information that is particular to the managed domain. It offers details of a specific topology or set of topologies that is a part of the data center scope.

The various scopes that are available on the Cisco Data Center Network Manager (DCNM) web interface are:

- **Data Center**
- **Default_SAN**
- **Default_LAN**
- Each SAN Fabric
- Custom scopes that you create

From the left menu bar, choose **Dashboard**. The **Dashboard** window displays the default dashlets.

The following are the default dashlets that appear in the **Dashboard** window:

- Data Center
- Inventory - Switches
- Inventory - Modules
- Top CPU
- Top ISLs/Trunks
- Link Traffic
- Alarms

- Events
- Server Status
- Audit Log

From the **Dashlets** drop-down list, you can choose more dashlets so that they are added to the dashboard.

The panels can be added, removed, and dragged around to reorder.

Dashlets

By default, a subset of the available dashlets is automatically displayed in the dashboard. To add a dashlet that is not automatically displayed in a dashboard, from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Dashboard**.

Step 2 From the **Dashlets** drop-down list, choose the dashlet that you want to add in the dashboard.

In the **Dashlets** drop-down list, an icon appears before the selected dashlet.

The following table lists the dashlets that you can add on the **Dashboard** window.

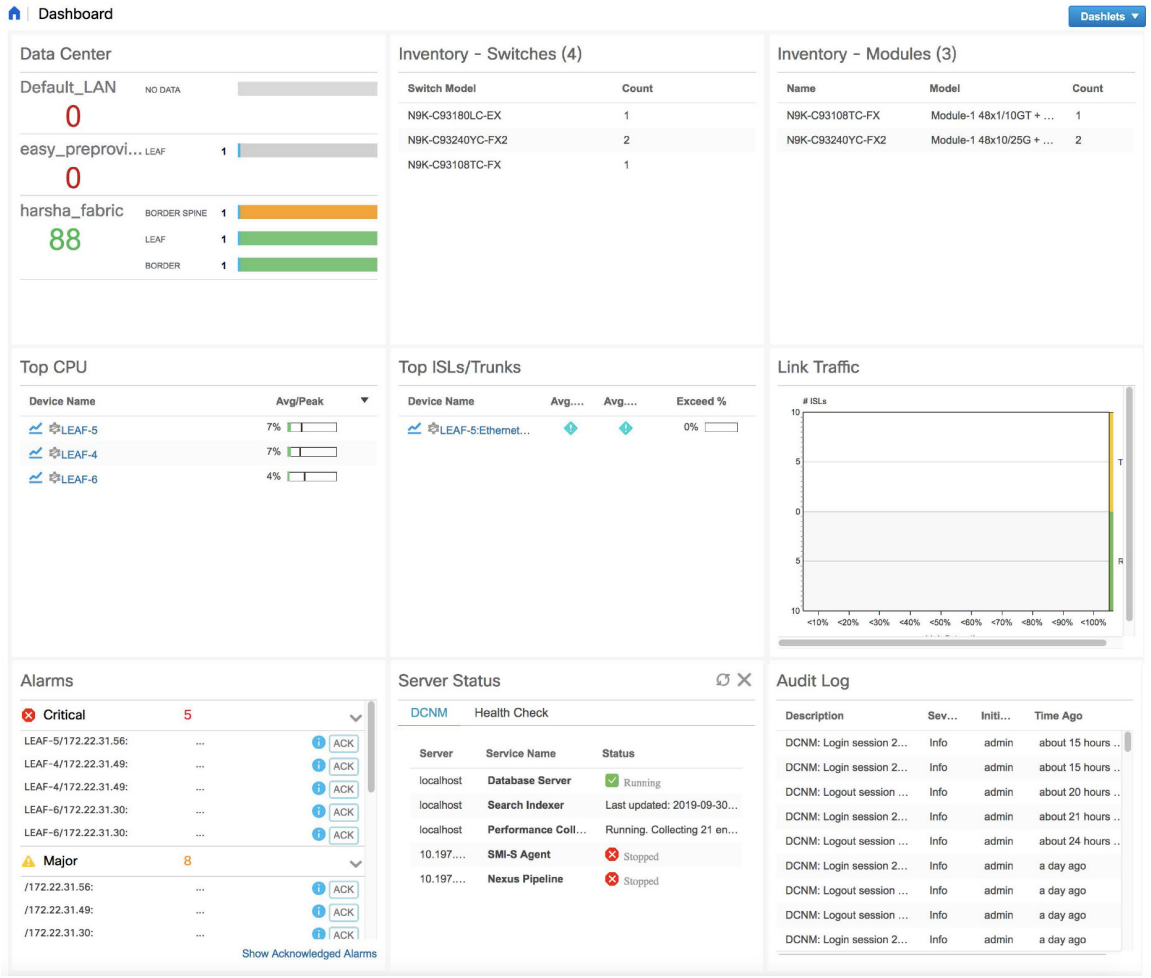
Dashlet	Description
Events	Displays events with **Critical**, **Error**, and **Warning** severity. In this dashlet, click the **Show Acknowledged Events** link to go to the **Monitor** > **Switch** > **Events**.
Alarms	Displays alarms with **Critical, Major, Minor**, and **Warning** severity. In this dashlet, click the **Show Acknowledged Alarms** link to go to the **Monitor** > **Alarms** > **View** window. Hover the mouse cursor over the blue **i** icon for more information about a specific alarm. Click **ACK** to acknowledge a specific alarm.
Link Traffic	Displays a diagram of Inter-Switch Link (ISL) and saturation link for transmitting and receiving in the data center.
Data Center	Displays the number of access, spine and leaf devices, and a generic health score for each switch group in the current scope. Devices are aggregated by type within a switch group.
Audit Log	Displays the accounting log table of Cisco DCNM.
Network Map	Displays the populated switch groups that are visible in your Role Based Access Control (RBAC) scope on

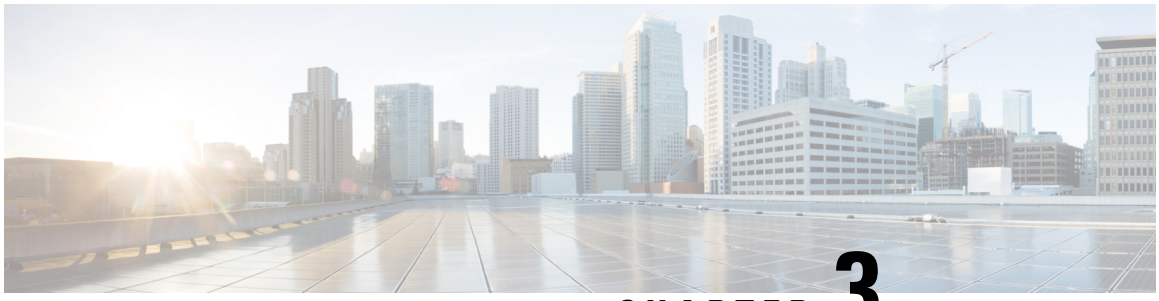
Dashlet	Description
	a world map. If you use the scope selector, it limits the set of switch groups displayed. If you click detach option, the map opens in a new tab and can be configured. • The network map dialog box has properties that are different from the Summary dashboard view: • You can click and drag nodes to move them around the map. The map saves their new positions. • You can double click a node to trigger a slider that contains the summary inventory information pertaining to a specific switch group. • You can upload an image of your choice as the background to the network map. **Note** You will be prompted to upload an image file with recommended dimension, which is the current window size. Reset returns the network map to its default state, resetting the position of the nodes and clearing the custom image.
Server Status	Displays the status of DCNM and federation servers, and the health check status for the components. The following services, server, and status details are displayed under the **DCNM** tab. • Database Server • Search Indexer • Performance Collector • NTPD Server • DHCP Server • SNMP Traps • Syslog Server The following component status and details are displayed under the **Health Check** tab. • AMQP Server • DHCP Server • TFTP Server • EPLS

Dashlet	Description
	• EPLC
Top ISLs/Trunks	Displays the performance data for the top ten performing ISLs, trunk ports or both. Each entry shows the current average receive and transmit percentage, with a graph depicting the percentage of time each trunk spent exceeding the currently configured thresholds.
Top SAN End Ports (SAN only)	Displays the performance data for the top ten performing SAN host and storage ports. Each entry shows the current receive and transmit percentage, with a graph depicting the percentage of time each trunk spent exceeding the currently configured thresholds. **Note** This dashlet is only for SAN.
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.
Top Temperature	Displays the module temperature sensor details of switches. **Note** This dashlet is only for LAN.
Health	Displays the health summary that contains two columns displaying the summary of problems and summary of events for the past 24 hours. Click the count adjacent to the warnings pertaining to switches, ISLs, hosts, or storage (other than 0) to view the corresponding inventory for that fabric. Click the count adjacent to the event severity levels (Emergency, Alert, Critical, Error, Warning, Notice, Info, or Debug) to view a summary of the corresponding events and descriptions.
Errors	Displays the error packets for the selected interface. This information is retrieved from the **Errors > In-Peak** and **Errors > Out-Peak** columns of the **Monitor > LAN / Ethernet** page.
Discards	Displays the error packets that are discarded for the selected interface. **Note** The Discards dashlet is only for LAN.
Inventory (Ports)	Displays the ports inventory summary information.

Dashlet	Description
Inventory (Modules)	Displays the switches on which the modules are discovered, the models name and the count.
Inventory (ISLs)	Displays the ISLs inventory summary information, such as the category and count of ISLs.
Inventory (Logical)	Displays the logical inventory summary information, such as the category and count of logical links.
Inventory (Switches)	Displays the switches inventory summary information such as the switch models and the corresponding count.
Inventory (Port Capacity)	Displays the port capacity inventory summary information such as the tiers, the number and percentage of the available ports, and the remaining days.

Note To restore the default dashlets in the dashboard page, click the **Default Set** link in the **Dashlet** drop-down list.


Dashboard
Dashlets
Data Center
Default_LAN
NO DATA
0
easy_preprovi...
LEAF
1
0
harsha_fabric
BORDER SPINE
1
88
LEAF
1
BORDER
1
Inventory - Switches (4)
Switch Model
Count
N9K-C93180LC-EX
1
N9K-C93240YC-FX2
2
N9K-C93108TC-FX
1
Inventory - Modules (3)
Name
Model
Count
N9K-C93108TC-FX
Module-1 48x1/10GT + ...
1
N9K-C93240YC-FX2
Module-1 48x10/25G + ...
2
Top CPU
Device Name
Avg/Peak
LEAF-5
7%
LEAF-4
7%
LEAF-6
4%
Top ISLs/Trunks
Device Name
Avg....
Avg....
Exceed %
LEAF-5:Ethernet...
0%
Link Traffic
ISLs
10
5
0
5
10
<10%
<20%
<30%
<40%
<50%
<60%
<70%
<80%
<90%
<100%
Alarms
Critical
5
LEAF-5/172.22.31.56:
LEAF-4/172.22.31.49:
LEAF-4/172.22.31.49:
LEAF-6/172.22.31.30:
LEAF-6/172.22.31.30:
ACK
Major
8
/172.22.31.56:
/172.22.31.49:
/172.22.31.30:
Show Acknowledged Alarms
Server Status
DCNM
Health Check
Server
Service Name
Status
localhost
Database Server
Running
localhost
Search Indexer
Last updated: 2019-09-30...
localhost
Performance Coll...
Running. Collecting 21 en...
10.197....
SMI-S Agent
Stopped
10.197....
Nexus Pipeline
Stopped
Audit Log
Description
Sev...
Initi...
Time Ago
DCNM: Login session 2...
Info
admin
about 15 hours ..
DCNM: Login session 2...
Info
admin
about 15 hours ..
DCNM: Logout session ...
Info
admin
about 20 hours ..
DCNM: Login session 2...
Info
admin
about 21 hours ..
DCNM: Logout session ...
Info
admin
about 24 hours ..
DCNM: Login session 2...
Info
admin
a day ago
DCNM: Logout session ...
Info
admin
a day ago
DCNM: Logout session ...
Info
admin
a day ago
DCNM: Login session 2...
Info
admin
a day ago



CHAPTER 3

Inventory

This chapter contains the following topics:

- Viewing Inventory Information, on page 13
- Discovery, on page 35

Viewing Inventory Information

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

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

Note You can use the **Print** icon to print the information that is displayed or you can also use the **Export** icon to export the information that is displayed to a Microsoft Excel spreadsheet. You can also choose the column that you want to display.

The Inventory menu includes the following submenus:

Viewing Inventory Information for Switches

To view the inventory information for switches from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory > View > Switches**.

The **Switches** window with a list of all the switches for a selected Scope is displayed.

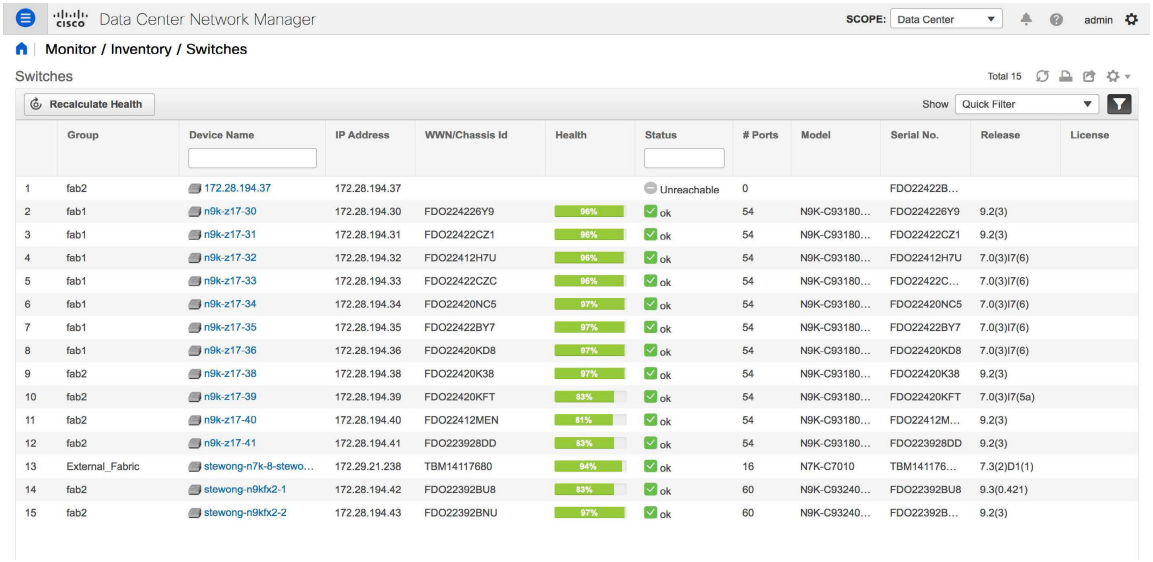
Step 2 You can also view the following information.

- **Group** column displays the switch group to which the switch belongs.
- In the **Device Name** column, select a switch to display the Switch Dashboard.

- **IP Address** column displays the IP address of the switch.
- **WWN/Chassis ID** displays the Worldwide Name (WWN) if available or chassis ID.
- **Health** displays the health situation of the switch.

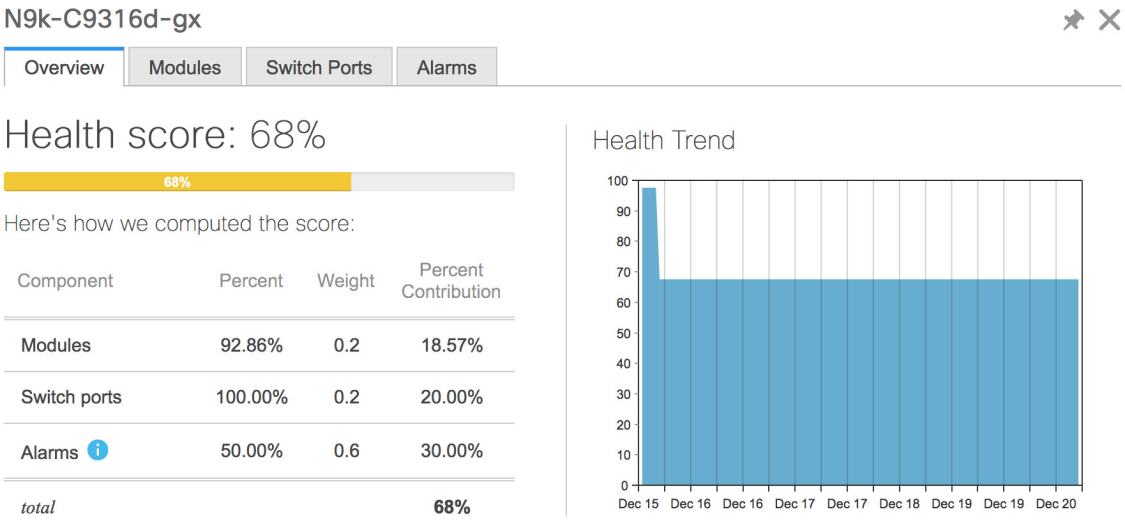
  Note To refresh and recalculate the latest health data for all the switches on Cisco DCNM, click the **Recalculate Health** button above the switches table.

- **Status** column displays the status of the switch.
- **# Ports** column displays the number of ports.
- **Model** column displays the model name of the switch.
- **Serial No.** column displays the serial number of the switch.
- **Release** column displays the switch version.
- **License** column displays the DCNM license that is installed on the switch.
- **Up Time** column displays the time period for which the switch is active.

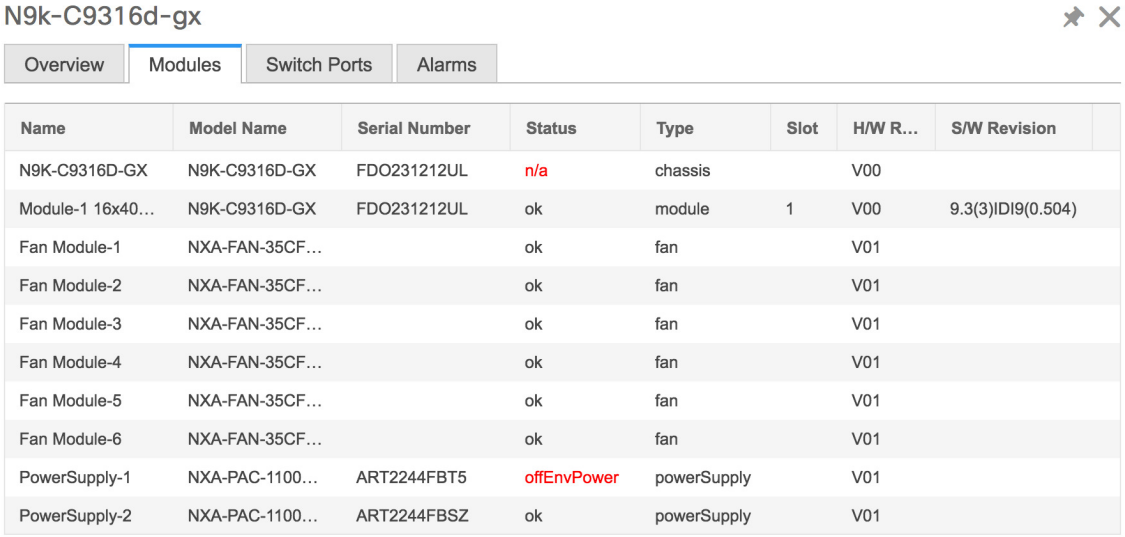


	Group	Device Name	IP Address	WWN/Chassis Id	Health	Status	# Ports	Model	Serial No.	Release	License
1	fab2	172.28.194.37	172.28.194.37			Unreachable	0		FDO22422B...		
2	fab1	n9k-z17-30	172.28.194.30	FDO224226Y9	96%	ok	54	N9K-C93180...	FDO224226Y9	9.2(3)	
3	fab1	n9k-z17-31	172.28.194.31	FDO22422CZ1	96%	ok	54	N9K-C93180...	FDO22422CZ1	9.2(3)	
4	fab1	n9k-z17-32	172.28.194.32	FDO22412H7U	96%	ok	54	N9K-C93180...	FDO22412H7U	7.0(3)I7(6)	
5	fab1	n9k-z17-33	172.28.194.33	FDO22422CZC	96%	ok	54	N9K-C93180...	FDO22422C...	7.0(3)I7(6)	
6	fab1	n9k-z17-34	172.28.194.34	FDO22420NC5	97%	ok	54	N9K-C93180...	FDO22420NC5	7.0(3)I7(6)	
7	fab1	n9k-z17-35	172.28.194.35	FDO22422BY7	97%	ok	54	N9K-C93180...	FDO22422BY7	7.0(3)I7(6)	
8	fab1	n9k-z17-36	172.28.194.36	FDO22420KD8	97%	ok	54	N9K-C93180...	FDO22420KD8	7.0(3)I7(6)	
9	fab2	n9k-z17-38	172.28.194.38	FDO22420K38	97%	ok	54	N9K-C93180...	FDO22420K38	9.2(3)	
10	fab2	n9k-z17-39	172.28.194.39	FDO22420KFT	83%	ok	54	N9K-C93180...	FDO22420KFT	7.0(3)I7(5a)	
11	fab2	n9k-z17-40	172.28.194.40	FDO22412MEN	81%	ok	54	N9K-C93180...	FDO22412M...	9.2(3)	
12	fab2	n9k-z17-41	172.28.194.41	FDO223928DD	83%	ok	54	N9K-C93180...	FDO223928DD	9.2(3)	
13	External_Fabric	stewong-n7k-8-stewo...	172.29.21.238	TBM14117680	94%	ok	16	N7K-C7010	TBM141176...	7.3(2)D1(1)	
14	fab2	stewong-n9kfx2-1	172.28.194.42	FDO22392BU8	83%	ok	60	N9K-C93240...	FDO22392BU8	9.3(0.421)	
15	fab2	stewong-n9kfx2-2	172.28.194.43	FDO22392BNU	97%	ok	60	N9K-C93240...	FDO22392B...	9.2(3)	

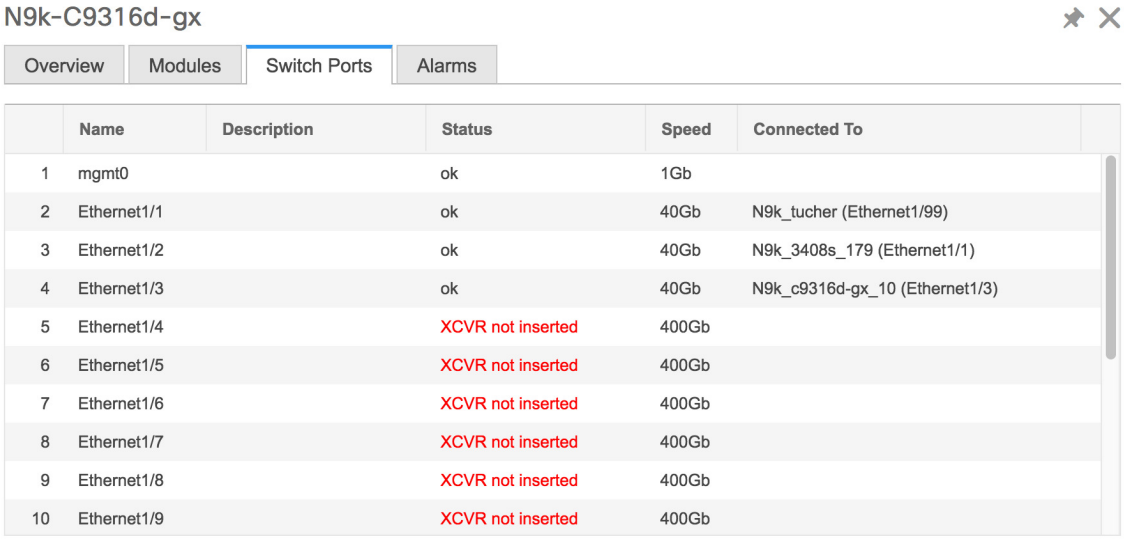
Step 3 Click **Health** to access the Health score window for a device. The Health score window includes health score calculation and health trend. The Overview tab displays the overall health score. All the modules, switch ports and alarms are taken into consideration while calculating the health score. Hover over the graph under Health Trend for detailed information on specific dates. Hover over the info icon next to Alarms to display the number of Critical, Major, Minor, and Warning alarms that have been generated.



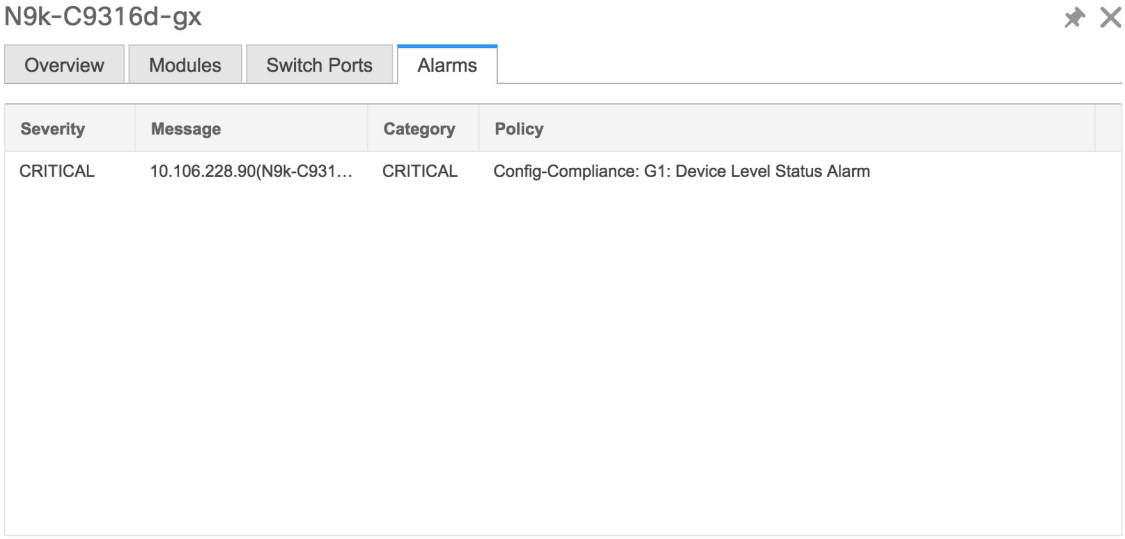
Click the **Modules** tab to display information about the various modules in the device. This tab displays information such as Name, Model name, Serial number, Status, Type, Slot, Hardware revision and Software revision.



Click the **Switch Ports** tab to display information about the device ports. This tab displays information such as Name, Description, Status, Speed, and the device to which a port is connected .



Click the **Alarms** tab to display information about the alarms that have been generated. This tab displays information such as alarm Severity, Message, Category, and the Policy that has been activated due to which the alarm is generated.



In the **Health** column, the switch health is calculated by the capacity manager based on the following parameters:

- Total number of modules
- Total number of modules impacted by the warning
- Total number of switch ports
- Total number of switch ports impacted by the warning

- Total number of critical severity alarms
- Total number of warning severity alarms
- Total number of major severity alarms
- Total number of minor severity alarms

Step 4 The value in the **Health** column is calculated based on the following:

- Percentage of modules impacted by warnings (Contributes 20% of the total health).
- Percentage of ports impacted by warnings (Contributes 20% of the total health).
- Percentage of alarms (Contributes 60% of the total health). The critical alarms contribute the highest value to this percentage followed by major alarms, minor alarms and warning alarms.

You may also have your own health calculation formula by implementing the common interface class: com.cisco.dcbu.sm.common.rif.HealthCalculatorRif.

The default Java class is defined as: health.calculator=com.cisco.dcbu.sm.common.util.HealthCalculatorAlarms.

- 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 daily cycle.
- If the switch is unlicensed, click **Unlicensed** in the DCNM License column. The **Administration > 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

Starting from Cisco DCNM 11.3(1) Release, you can view information about switch health along with the switch summary by clicking on a switch in the **Topology** window or by choosing **Control>Fabrics>Fabric Builder**, selecting a fabric and clicking on a switch in the **Fabric Builder** window.

Viewing System Information

The switch dashboard displays the details of the selected switch.

Procedure

Step 1 From the Cisco DCNM home page, choose **Inventory > View > Switches**.

An inventory of all the switches that are discovered by Cisco DCNM Web UI is displayed.

Step 2 Click a switch in the **Device Name** column.

The **Switch** dashboard that corresponds to that switch is displayed along with the following information:

Step 3 Click the **System Information** tab. This tab displays detailed system information such as group name, health, module, time when system is up, serial number, the version number, contact, location, DCNM license, status, system log sending status, CPU and memory utilization, and VTEP IP address are displayed. Click **Health** to access the Health score screen, which includes health score calculation and health trend. The popup contains Overview, Modules, Switch Ports, and Events tabs.

- (Optional) Click **SSH** to access the switch through Secure Shell (SSH).
- (Optional) Click **Device Manager** to view a graphical representation of a Cisco MDS 9000 Family switch chassis, a Cisco Nexus 5000 Series switch chassis, a Cisco Nexus 7000 Series switch chassis, or a Cisco Nexus 9000 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.
- (Optional) Click **HTTP** to access the switch through Hypertext Transfer Protocol (HTTP) for that switch.
- (Optional) Click **Accounting** to go to the Viewing Accounting Information window pertaining to this switch.
- (Optional) Click **Backup** to go to the Viewing a Configuration window.
- (Optional) Click **Events** to go to the Viewing Events Registration, on page 228 window.
- (Optional) Click **Show Commands** to display the device show commands. The Device Show Commands page helps you to view commands and execute them.
- (Optional) Click **Copy Running Config to Startup Config** to copy the running configuration to the startup configuration.

Interfaces

Adding Interfaces

To add the interfaces from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.

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

Step 2 In the **Device Name** column, select a switch to display **Switch Dashboard**.

Step 3 Click the **Interfaces** tab.

Step 4 Click **Add** to add a logical interface. The **Add Interface** window appears.
If you want to add a sub-interface, you select an interface and click **Add**.

Step 5 In the **Type** field, choose the type of the interface. For example, VLAN, loopback, NVE.

Step 6 In the **Number** field, specify the interface number.

Step 7 Select the **Admin State ON** check box to specify whether the interface is shut down or not.

Editing Interfaces

To edit the interfaces from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.
You see the Switches window displaying a list of all the switches for a selected Scope.

Step 2 In the **Device Name** column, select a switch to display **Switch Dashboard**.

Step 3 Click the **Interfaces** tab.

Step 4 Click **Edit** to edit an interface. The variables that are shown in the **Edit Configuration** window are based on the template and its policy.

- The **Admin State ON** check box in the **Edit Configuration** window indicates whether the interface is shut down or not.
- The **Clear Config** before the deployment check box helps you to set a port to its default configuration. When there is a set of configurations already available on the port and these configurations conflict with the configurations that want to place on the port, you may need to clear the configurations before the deployment.
- In the **Preview** window, the left pane shows the configurations that the template generated based on your input, whereas the right pane shows the configurations that are currently available on the switch.

Deleting Interfaces

To delete the interfaces from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.

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

Step 2 In the **Device Name** column, select a switch to display **Switch Dashboard**.

Step 3 Click the **Interfaces** tab.

Step 4 Click **Delete** to add a logical interface.

Shutting Down and Bring Up Interfaces

To shut down and bring up the interfaces from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.
The **Switches** window is displayed with a list of all the switches for a selected **Scope**.

Step 2 In the **Device Name** column, select a switch to display **Switch Dashboard**.

Step 3 Click the **Interfaces** tab.

Step 4 Click **Shutdown** to disable an interface. For example, you may want to isolate a host from the network or a host that is not active in the network.

To enable an interface, Click **No Shutdown** button.

Displaying Interface Show Commands

To display interface show commands from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.
You see the **Switches** window displaying a list of all the switches for a selected **Scope**.

Step 2 In the **Device Name** column, select a switch to display **Switch Dashboard**.

Step 3 Click the **Interfaces** tab.

Step 4 Click **Show** to display the interface show commands.

The **Interface Show Commands** window helps you to view commands and execute them.

Rediscovering Interfaces

To rediscover interfaces from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.

The **Switches** window is displayed showing a list of all the switches for a selected **Scope**.

Step 2 In the **Device Name** column, select a switch to display **Switch Dashboard**.

Step 3 Click the **Interfaces** tab.

Step 4 Click **Rediscover** to rediscover the selected interfaces. For example, after you edit or enable an interface, you can rediscover the interface.

Viewing Interface History

To view the interface history from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Switches**.

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

Step 2 In the **Device Name** column, select a switch to display **Switch Dashboard**.

Step 3 Click the **Interfaces** tab.

Step 4 Click **Interface History** to display the interface history details such as **Policy Name**, **Time of Execution**, and so on.

VLAN

You create a VLAN by assigning a number to it; you can delete VLANs and move them from the active operational state to the suspended operational state.

To configure VLANs, choose **Inventory > View > Switches**, and then click a switch in the **Device Name** column.

The following table describes the buttons that appear on this page.

Table 2: VLAN Tab

Field	Description
Clear Selections	Allows you to unselect all the VLANs that you selected.
Add	Allows you to create Classical Ethernet or Fabric Path VLANs.
Edit	Allows you to edit a VLAN.
Delete	Allows you to delete a VLAN.
No Shutdown	Allows you to enable a VLAN.
Shutdown	Allows you to disable a VLAN.
Show	Allows you to display the VLAN show commands.

This section contains the following:

Adding a VLAN

To add a VLAN from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory > View > Switches**.

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

Step 2 In the **Device Name** column, select a switch to display the **Switch Dashboard**.

Step 3 Click the **VLAN** tab.

Step 4 Click **Add** to create Classical Ethernet or Fabric Path VLANs. In the **Add VLAN** window, specify the following fields:

a) In the **Vlan Id** field, enter the VLAN ID.

b) In the **Mode** field, specify whether you are adding Classical Ethernet or Fabric Path VLAN.
c) Select the **Admin State ON** check box to specify whether the VLAN is shut down or not.

Editing a VLAN

To edit a VLAN from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory > View > Switches**.

The **Switches** window is displayed with a list of all the switches for a selected **Scope**.

Step 2 In the **Device Name** column, select a switch to display the **Switch Dashboard**.

Step 3 Select one or more VLANs, and then click the **Edit**.

Deleting a VLAN

To delete a VLAN from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory > View > Switches**.

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

Step 2 In the **Device Name** column, select a switch to display the **Switch Dashboard**.

Step 3 Click **VLAN** tab.

Step 4 Select the VLAN that you want to delete, and then click **Delete**.

Shutting Down a VLAN

To shut down a VLAN from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory > View > Switches**.

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

Step 2 In the **Device Name** column, select a switch to display **Switch Dashboard**.

Step 3 Click the **VLAN** tab.

Step 4 Click **Shutdown** to disable a VLAN.

To enable a VLAN, click **No Shutdown** button. For example, if you want to start traffic flow on a VLAN you can enable it.

Displaying VLAN Show Commands

To display VLAN show commands from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory > View > Switches**.

The **Switches** window is displayed, showing a list of all the switches for a selected **Scope**.

Step 2 In the **Device Name** column, select a switch to display **Switch Dashboard**.

Step 3 Click the **VLAN** tab.

Step 4 Click **Show** to display the VLAN show commands. Based on the VLAN selection, you can show the VLAN commands. **Interface Show Commands** window displays the commands and allows you to execute them.

FEX

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. 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.

Note FEX feature is available on LAN devices only. Therefore, you will see FEX on Cisco DCNM **Inventory Switches**. FEX is also not supported on Cisco Nexus 1000V devices.

Note 4x10G breakout for FEX connectivity is not supported on Cisco Nexus 9500 Switches.

Note The Fabric Extender may connect to the switch through several separate physical Ethernet interfaces or at most one port channel interface.

This section describes how to manage Fabric Extender (FEX) on Cisco Nexus Switches through Cisco DCNM.

You can create and manage FEX from Cisco DCNM **Inventory > Switches**.

Note FEX tab is visible only if you choose a LAN device.

The following table describes the fields that appear on this page.

Table 3: FEX Operations

Field	Description
Add	Click to add a new FEX to a Cisco Nexus Switch.
Edit	Select any active FEX radio button and click Edit to edit the FEX configuration. You can create an edit template and use it for editing FEX. Select template type as POLICY and sub type as FEX.
Delete	Select the FEX radio button, and click Delete icon to delete the FEX associated with the switch.
Show	Allows you to view various configuration details for the selected FEX ID. You can select the following from the drop-down list. • show_diagnostic • show_fex • show_fex_detail • show_fex_fabric • show_fex_inventory • show_fex_module The variables for respective show commands are displayed in the Variables area. Review the Variables and click **Execute**. The output appears in the **Output** area. You can create a show template for FEX. Select template type as SHOW and sub type as FEX.
FEX History	Allows you to view the history of the FEX configuration tasks for a particular FEX. You can review the Event Type, Policy Name, Status, Time of Execution, User Name for the selected FEX.

Table 4: FEX Field and Description

Field	Description
Fex Id	Uniquely identifies a Fabric Extender that is connected to a Cisco NX-OS device.
Fex Description	Description that is configured for the Fabric Extender.

Field	Description
Fex Version	Specifies the version of the FEX that is associated with the switch.
Pinning	An integer value that denotes the maximum pinning uplinks of the Fabric Extender that is active at a time.
State	Specifies the status of the FEX as associated with the Cisco Nexus Switch.
Model	Specifies the model of the FEX.
Serial No.	Specifies the configured serial number. **Note** If this configured serial number and the serial number of the Fabric Extender are not the same, the Fabric Extender will not be active.
Port Channel	Specifies the port channel number to which the FEX is physically connected to the Switch.
Ethernet	Refers to the physical interfaces to which the FEX is connected.
vPC ID	Specifies the vPC ID configured for FEX.

This chapter includes the following sections:

Add FEX

To add single-home FEX from the Cisco DCNM Web UI, perform the following steps:

Before you begin

You can add a Fabric Extender (FEX) to the Cisco Nexus Switches through the Cisco DCNM Web Client. If the FEX is physically connected to the switch, FEX will become online after it is added. If the FEX is not physically connected to the switch, the configuration is deployed to the switch, which in turn enables FEX when connected.



Note You can create only single homed FEX through **Inventory > Switches > FEX > Add FEX**. To create a dual-homed FEX, use the vPC wizard through **Configure > Deploy > vPC**.

Ensure that you have successfully discovered LAN devices and configured LAN credentials before you configure FEX.

Procedure

Step 1 Choose **Inventory > Switches > FEX**.

The **FEX** window is displayed.

Step 2 Click the **Add** FEX icon.

Step 3 In the General tab, in the **PORTCHANNEL** field, enter the interface port channel number which is connected to the FEX.

Step 4 In the **INT_RANGE** field, enter the interface range within which the FEX is connected to the switch.

Note Do not enter the interface range, if the interfaces are already a part of port channel.

Step 5 In the **FEX_ID** field, enter the ID for FEX that is connected to a Cisco NX-OS device.

The identifier must be an integer value between 100 to 199.

Step 6 Click **Add**.

The configured Single-home FEX appears in the list of FEXs associated to the device.

Edit FEX

To edit and deploy FEX from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **Switches** > **FEX**.

The **FEX** window is displayed.

Step 2 Select the FEX radio button that you must edit. Click **Edit** FEX icon.

Step 3 In the Edit Configuration window, from the Policy drop-down list, select **Edit_FEX** to edit the FEX configuration.

Step 4 Edit the **pinning** and **FEX_DESC** fields, as required.

Note If you initially configured port 33 on the parent switch as your only fabric interface, all 48 host interfaces are pinned to this port. If you provision another port, for example 35, then you must perform this procedure to redistribute the host interfaces. All host interfaces are brought down and host interfaces 1 to 24 are pinned to fabric interface 33 and host interfaces 25 to 48 are pinned to fabric interface 35.

Step 5 Click **Preview**.

You can view the generated configuration for the selected FEX ID. The following is a configuration example for FEX ID 101.

```
fex 101
pinning max-links 1
description test
```

Step 6 After you review the configuration summary on the Preview window, on the Edit Configuration screen, click **Deploy** to deploy the FEX for the switch.

VDCs

This section describes how to manage Virtual Device Contexts (VDCs) on Cisco Nexus 7000 Switches through Cisco DCNM.

Users with the network administrator (network-admin) role can create Virtual Device Contexts (VDCs). VDC resource templates limit the amount of physical device resources available to the VDC. The Cisco NX-OS software provides a default resource template, or you can create resource templates.

You can create and manage VDCs from Cisco DCNM **Inventory > Switches > VDCs**. As Cisco DCNM supports DCNM on Cisco Nexus 7000 Series only, click an active Cisco Nexus 7000 Switch. After you create a VDC, you can change the interface allocation, VDC resource limits, and the high availability (HA) policies.

The following table describes the fields that appear on this page.

Table 5: VDC Operations

Field	Description
Add	Click to add a new VDC.
Edit	Select any active VDC radio button and click Edit to edit the VDC configuration.
Delete	Allows you to delete the VDC. Select any active VDC radio button and click Delete to remove the VDC associated with the device.
Resume	Allows you to resume a suspended VDC.
Suspend	Allows you to suspend an active non-default VDC. Save the VDC running configuration to the startup configuration before suspending the VDC. Otherwise, you will lose the changes to the running configuration. **Note** You cannot suspend the default VDC. **Caution** Suspending a VDC disrupts all traffic on the VDC.
Rediscover	Allows you to resume a non-default VDC from the suspended state. The VDC resumes with the configuration that is saved in the startup configuration.
Show	Allows you to view the Interfaces and Resources that are allocated to the selected VDC. In the Interface tab, you can view the mode, admin-status, and operational status for each interface associated with the VDC. In the Resource tab, you can view the allocation of resources and current usage of these resources.

Table 6: Vdc Table Field and Description

Field	Description
Name	Displays the unique name for the VDC

Field	Description
Type	Species the type of VDC. The two types of VDCs are: • Ethernet • Storage
Status	Specifies the status of the VDC.
Resource Limit-Module Type	Displays the allocated resource limit and module type.
HA-Policy • Single Supervisor • Dual Supervisor	Specifies the action that the Cisco NX-OS software takes when an unrecoverable VDC fault occurs. You can specify the HA policies for single supervisor module and dual supervisor module configurations when you create the VDC. The HA policy options are as follows: **Single supervisor module configuration:** • Bringdown—Puts the VDC in the failed state. To recover from the failed state, you must reload the physical device. • Reload—Reloads the supervisor module. • Restart—Takes down the VDC processes and interfaces and restarts it using the startup configuration. **Dual supervisor module configuration:** • Bringdown—Puts the VDC in the failed state. To recover from the failed state, you must reload the physical device. • Restart—Takes down the VDC processes and interfaces and restarts it using the startup configuration. • Switchover—Initiates a supervisor module switchover. The default HA policies for a non-default VDC that you create is restart for a single supervisor module configuration and switchover for a dual supervisor module configuration. The default HA policy for the default VDC is reload for a single supervisor module configuration and switchover for a dual supervisor module configuration.
Mac Address	Specifies the default VDC management MAC address.

Field	Description
Management Interface • IP Address Prefix • Status	Species the IP Address of the VDC Management interface. The status shows if the interface if up or down.
SSH	Specifies the SSH status

Note If you change the VDC hostname of a neighbor device after initial configuration, the link to the old VDC hostname is not replaced with the new hostname automatically. As a workaround, we recommend manually deleting the link to the old VDC hostname.

This chapter includes the following sections:

Add VDCs

To add VDC from the Cisco DCNM Web UI, perform the following steps:

Before you begin

Ensure that you have discovered the physical device using a username that has the network-admin role.

Obtain an IPv4 or IPv6 address for the management interface (mgmt 0) if you want to use out-of-band management for the VDC.

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.

Procedure

Step 1 Choose **Inventory** > **Switches** > **VDC**.

The **VDC** window is displayed.

Step 2 Click the **Add** VDC icon.

Step 3 From the drop-down list, select the VDC type.

You can configure the VDC in two modes.

- Configuring Ethernet VDCs
- Configuring Storage VDCs

The default VDC type is Ethernet.

Step 4 Click **OK**.

Configuring Ethernet VDCs

To configure VDC in Ethernet mode from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 In the General Parameter tab, specify the VDC **Name**, **Single supervisor HA-policy**, **Dual supervisor HA-policy**, and **Resource Limit - Module Type**.

Step 2 In the Allocate Interface tab, select the network interfaces (dedicated interfaces membership) to be allocated to the VDC.

Click **Next**.

Step 3 In the Allocate Resource tab, specify the resource limits for the VDC.

Select the radio button and choose **Select a Template from existing Templates** or **Create a New Resource Template**. VDC resource templates describe the minimum and maximum resources that the VDC can use. If you do not specify a VDC resource template when you create a VDC, the Cisco NX-OS software uses the default template, vdc-default.

- If you choose Select a Template from existing Templates, from the **Template Name** drop-down list, you can select **None**, **global-default**, or **vdc-default**.

  The template resource limits are detailed in the following below:

Table 7: Template Resource Limits

Resource	Minimum	Maximum
Global Default VDC Template Resource Limits		
Anycast Bundled		
IPv6 multicast route memory	8	8 Route memory is in megabytes.
IPv4 multicast route memory	48	48
IPv6 unicast route memory	32	32
IPv4 unicast route memory		
VDC Default Template Resource Limits		
Monitor session extended		
Monitor session mx exception		
Monitor SRC INBAND		
Port Channels		
Monitor DST ERSPAN		
SPAN Sessions		

Resource	Minimum	Maximum
VLAN		
Anycast Bundled		
IPv6 multicast route memory		
IPv4 multicast route memory		
IPv6 unicast route memory		
IPv4 unicast route memory		
VRF		

- If you choose Create New Resource Template, enter a unique **Template Name**. In the Resource Limits area, enter the minimum and maximum limits, as required for the resources.

You can edit individual resource limits for a single VDC through the Cisco DCNM **Web Client > Inventory > Switches > VDC**.

Click **Next**.

Step 4 In the Authenticate tab, you can allow the Admin to configure the password and also authenticate users using AAA Server Groups.

In the Admin User Area:

- Check the **Enable Password Strength Check** checkbox, if necessary.
- In the **Password** field, enter the admin user password.
- In the **Confirm Password** field, reenter the admin user password.
- In the **Expiry Date** field, click the down arrow and choose an expiry date for the admin user from the Expiry Date dialog box. You can also select **Never** radio button not to expire the password.

In the AAA Server Groups area:

- In the **Group Name** field, enter an AAA server group name.
- In the **Servers** field, enter one or more host server IPv4 or IPv6 addresses or names, which are separated by commas.
- In the **Type** field, choose the type of server group from the drop-down list.

Click **Next**.

Step 5 In the Management Ip tab, enter IPv4 or IPv6 Address information.

Click **Next**.

Step 6 In the Summary tab, review the VDC configuration.

Click **Previous** to edit any parameters.

Click **Deploy** to configure VDC on the device.

Step 7 In the Deploy tab, the status of the VDC deployment is displayed.

A confirmation message appears. Click **Know More** to view the commands that are executed to deploy the VDC.

Click **Finish** to close the VDC configuration wizard and revert to view the list of VDCs configured on the device.

Configuring Storage VDCs

To configure VDCs in storage mode from the Cisco DCNM Web UI, perform the following steps:

Before you begin

Create a separate storage VDC when you run FCoE on the device. Only one of the VDCs can be a storage VDC, and the default VDC cannot be configured as a storage VDC.

You can configure shared interfaces that carry both Ethernet and Fibre Channel traffic. In this specific case, the same interface belongs to more than one VDC. The shared interface is allocated to both an Ethernet and a storage VDC.

Procedure

Step 1 In the General Parameter tab, specify the VDC **Name**, **Single supervisor HA-policy**, **Dual supervisor HA-policy**, and **Resource Limit - Module Type**.

Step 2 In the Allocate FCoE Vlan tab, select the available **Ethernet Vdc** from the drop-down list.

The existing Ethernet VLANs range is displayed. Select **None** not to choose any available Ethernet VDCs.

You can allocate specified FCoE VLANs to the storage VDC and specified interfaces.

Click **Next**.

Step 3 In the Allocate Interface tab, add the dedicated and shared interfaces to the FCoE VDC.

Note The dedicated interface carries only FCoE traffic and the shared interface carries both the Ethernet and the FCoE traffic.

You can configure shared interfaces that carry both Ethernet and Fibre Channel traffic. In this specific case, the same interface belongs to more than one VDC. FCoE VLAN and shared interface can be allocated from same Ethernet VDC.

Click **Next**.

Step 4 In the Authenticate tab, you can allow the Admin to configure the password and also authenticate users using AAA Server Groups.

In the Admin User Area:

- Check the **Enable Password Strength Check** checkbox, if necessary.
- In the **Password** field, enter the admin user password.
- In the **Confirm Password** field, reenter the admin user password.

- In the **Expiry Date** field, click the down arrow and choose an expiry date for the admin user from the Expiry Date dialog box. You can also select **Never** radio button not to expire the password.

In the AAA Server Groups area:

- In the **Group Name** field, enter an AAA server group name.
- In the **Servers** field, enter one or more host server IPv4 or IPv6 addresses or names, which are separated by commas.
- In the **Type** field, choose the type of server group from the drop-down list.

Click **Next**.

Step 5 In the Management Ip tab, enter IPv4 or IPv6 Address information.

Click **Next**.

Step 6 In the Summary tab, review the VDC configuration.

Click **Previous** to edit any parameters.

Click **Deploy** to configure VDC on the device.

Step 7 In the Deploy tab, the status of the VDC deployment is displayed.

A confirmation message appears. Click **Know More** to view the commands that are executed to deploy the VDC.

Click **Finish** to close the VDC configuration wizard and revert to view the list of VDCs configured on the device.

Edit VDC

To edit VDC from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **Switches** > **VDC**.

The **VDC** window is displayed.

Step 2 Select the VDC radio button that you must edit. Click the **Edit** VDC icon.

Step 3 Modify the parameters as required.

Step 4 After you review the configuration summary on the Summary tab, click **Deploy** the VDC with the new configuration.

Viewing Inventory Information for Modules

To view the inventory information for modules from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Modules**.

The **Modules** window is displayed with a list of all the switches and its details for a selected Scope.

Step 2 You can view the following information.

- **Group** column displays the group name of the module.
- **Switch** column displays the switch name on which the module is discovered.
- **Name** displays the module name.
- **ModelName** displays the model name.
- **SerialNum** column displays the serial number.
- **2nd SerialNum** column displays the second serial number.
- **Type** column displays the type of the module.
- **Slot** column displays the slot number.
- **Hardware Revision** column displays the hardware version of the module.
- **Software Revision** column displays the software version of the module.
- **Asset ID** column displays the asset id of the module.
- **OperStatus** column displays the operation status of the module.
- **IO FPGA** column displays the IO field programmable gate arrays (FPGA) version.
- **MI FPGA** column displays the MI field programmable gate arrays (FPGA) version.

Viewing Inventory Information for Licenses

To view the inventory information for licenses from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory** > **View** > **Licenses**.

The **Licenses** window is displayed based on the selected Scope.

Step 2 You can view the following information.

- **Group** column displays the group name of switches.
- **Switch** column displays the switch name on which the feature is enabled.
- **Feature** displays the installed feature.

- **Status** displays the usage status of the license.
- **Type** column displays the type of the license.
- **Warnings** column displays the warning message.

Discovery

Starting from Cisco DCNM release 10.x, Cisco DCNM Web Client allows the **admin** to associate **user** to one or more device scope or group. That means you can only access and configure the associated group or scope devices based on Role Based Access Control (RBAC). Though you might not have the access to other users' associated devices, you can still see all the discovered devices under the **Inventory > Discovery** tab.

From the left menu bar, go to **Administration > Management Users**. You can create users and associate groups, manage remote authentication, and see all the connected clients. For more information about RBAC, navigate to Managing Local Users.

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

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

Tip If the discovered Device is not in the scope of the current user the check box for the LAN Device in the LAN table grays out.

This section contains the following:

Adding LAN Switches

To add LAN switches from the Cisco DCNM Web UI, perform the following steps.

For any switch to be successfully imported into DCNM, the user defined on the switch via local or remote AAA, and used for import into DCNM should have the following permissions:

- SSH access to the switch
- Ability to perform SNMPv3 queries
- Ability to run **show** commands

Procedure

Step 1 Choose **Inventory > Discovery > LAN** Switches.

You see the list of LAN devices in the **Switch** column.

Step 2 Click the **Add** icon to add LAN.

You see the **Add LAN Devices**dialog box.

Step 3 Select **Hops from seed Switch** or **Switch List**. The fields vary depending on your selection.

Step 4 Enter the **Seed Switch** IP address for the fabric.

For LAN Switches Discovery, DCNM allow both IPv4 and IPv6 address for the Seed Switch.

Step 5 The options vary depending on the discovery type selected. For example, if you check **Use SNMPv3/SSH**, varied fields are displayed.

Step 6 Click the drop-down list and choose **Auth-Privacy** security level.

Step 7 Enter the **Community**, or user credentials.

Step 8 Select the LAN group from the LAN groups candidates which is in the scope of the current user.

Note Select DCNM server and click **Add** to add LAN switches.

Step 9 Click **Next** to begin the shallow discovery.

Step 10 In the **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 **timeout** or **Cannot be contacted**, these switches cannot be added. Only the switches that are reachable and not managed yet are available to select. The checkbox is disabled for the switches that are not available
- When you add or discover LAN devices in DCNM, java is used as a part of the discovery process. If firewall blocks the process then it uses TCP connection port 7 as a discovery process. Ensure that the **cdp.discoverPingDisable** server property is set to **true**. Choose **Web UI > Administration > DCNM Server > Server Properties** to set the server property.

Step 11 Select a switch and click **Add** to add a switch to the switch group.

If one of more seed switches is not reachable, it is shown as “unknown” on the shallow Discovery window.

Editing LAN Devices

To edit LAN devices from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Inventory > Discovery > LAN Switches**.

Step 2 Select the check box next to the LAN that you want to edit and click **Edit** icon.

You see the **Edit LAN** dialog box.

Step 3 Enter the **Username** and **Password**.

Note Select **Credential** or **Management State** to change the Credential or Management state. If **Credential** is selected, you can change the SNMP version and Auth-Privacy if v3, username or password. If **Management State** is selected, you can change the status to managed or unmanaged.

Step 4 Select the LAN status as **Managed** or **Unmanaged**.

Step 5 Click **Apply** to save the changes.

Removing LAN Devices from Cisco DCNM

You can remove a LAN switch from Cisco DCNM.

Procedure

Step 1 Choose **Inventory > Discovery > LAN Switches**.

Step 2 Select the check box next to the LAN that you want to remove and click **Delete** to remove the switches and all their data.

Step 3 Click **Yes** to review the LAN device.

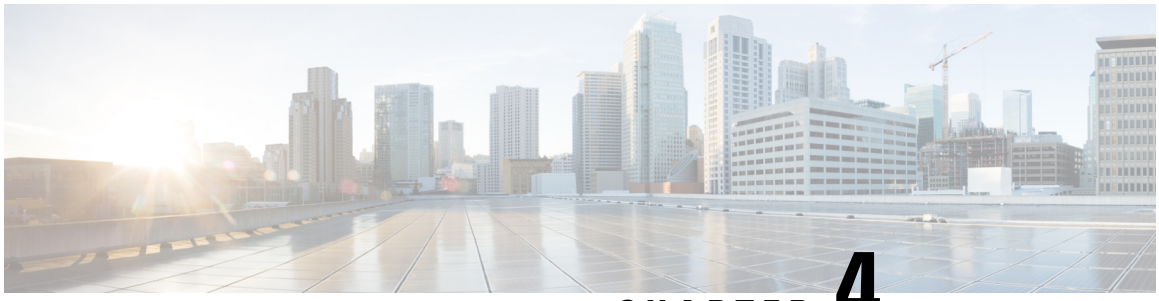
Rediscover LAN Task

Procedure

Step 1 Choose **Inventory > Discovery > LAN Switches**.

Step 2 Click **Rediscover LAN**.

Step 3 Click **Yes** in the pop-up window to rediscover the LAN.



CHAPTER 4

Monitor

This chapter contains the following topics:

- Monitoring Switch, on page 39
- Monitoring LAN, on page 42
- Alarms, on page 46

Monitoring Switch

The Switch menu includes the following submenus:

Viewing Switch CPU Information

To view the switch CPU information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > Switch > CPU**.

The **CPU** window is displayed. This window displays the CPU information for the switches in that scope.

Step 2 You can use the drop-down to filter the view by Last 10 Minutes, Last Hour, Last Day, Last Week, Last Month, and Last 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 Last 10 Minutes, Last Hour, Last Day, Last Week, Last Month, and Last Year. You can choose the chart type and chart options to show as well.

Viewing Switch Memory Information

To view the switch memory information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > Switch > Memory**.

The memory panel is displayed. This panel displays the memory information for the switches in that scope.

Step 2 Use the drop-down to filter the view by Last 10 Minutes, Last Hour, Last Day, Last Week, Last Month, and Last Year.

Step 3 Click the chart icon in the **Switch** 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 memory utilization chart in varied views.

Viewing Switch Traffic and Errors Information

To view the switch traffic and errors information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > Switch > Traffic**.

The **Switch Traffic** panel is displayed. This panel displays the traffic on that device for the past 24 hours.

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

Step 3 Click the **Export** icon in the upper-right corner to export the data into a spreadsheet.

Step 4 Click **Save**.

Step 5 Click the switch name to view the Switch Dashboard section.

Viewing Switch Temperature

Cisco DCNM includes the module temperature sensor monitoring feature, using which you can view the sensor temperature of a switch. You can choose an interval by which to filter the sensor list. The default interval is **Last Day**. Only sensors that have historical temperature data is shown in the list. You can choose between Last ten Minutes, Last Hour, Last Day, Last Week, and Last Month.



Note It is not necessary to configure the LAN credentials under the **Configure > Credentials Management > LAN Credentials** screen to fetch the temperature monitoring data from the switches.

To view the switch temperature information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > Switch > Temperature**.

The **Switch Temperature** window is displayed with the following columns.

- **Scope**: The sensor belongs to a switch, which is part of a fabric. The fabric that it belongs to is shown as its scope. When the scope selector at the top of Cisco DCNM is used, the sensor list is filtered by that scope.
- **Switch**: Name of the switch the sensor belongs to.
- **IP Address**: IP Address of the switch.
- **Temperature Module**: The name of the sensor module.
- **Avg/Range**: The first number is the average temperature over the interval that is specified at the top of the table. The second set of numbers is the range of the temperature over that interval.
- **Peak**: The maximum temperature over the interval

Step 2 From this list, each row has a chart icon, which you can click.
A chart is displayed, which shows historical data for the sensor. The interval for this chart can be changed as well, between 24 hours, 1 week, and 1 month.

Enabling Temperature Monitoring

You can enable the temperature monitoring feature for LAN switches from the LAN Collections screen, and for the SAN switches by setting a few properties under Administration > DCNM Server > Server Properties screens.

Enabling Temperature Monitoring for LAN Switches

1. From the menu bar, choose **Administration > Performance Setup > LAN Collections**.
2. Select the **Temperature Sensor** check box.
3. Select the type of LAN switches for which you want to collect performance data.
4. Click **Apply** to save the configuration.

Viewing Accounting Information

To view the accounting information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > Switch > Accounting**.

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

Step 2 Select **Advanced Filter** beside the filter icon to search the accounting information by **Source**, **Username**,**Time**, and **Description**. Or select **Quick Filter** to search under each column.

Step 3 You can also select a row and click 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** icon to export the data to a Microsoft Excel spreadsheet.

Viewing Events Information

To view the events and syslog from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **Switch** > **Events**.

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

The **Count** column displays the number of times the same event has occurred during the time period as shown in the **Last Seen** and **First Seen** columns.

Click a switch name in the **Switch** column to view the switch dashboard.

Step 2 Select an event in the table and click the **Add Suppressor** icon to open the shortcut of adding an event suppressor rule.

Step 3 Select one or more events from the table and click the **Acknowledge** icon to acknowledge the event information for the fabric.

- After you acknowledge the event for a fabric, the acknowledge icon is displayed in the **Ack** column next to the fabric.

Step 4 Select the fabric and click the **Unacknowledge** icon to cancel an acknowledgment for a fabric.

Step 5 Select **Advanced Filter** beside the filter icon to search the accounting information by **Source**, **Username**,**Time**, and **Description**. Or select **Quick Filter** to search under each column.

Step 6 Select a fabric and use the **Delete** icon to delete the fabric and event information from the list.

Step 7 Click the **Print** icon to print the event details.

Step 8 Click the **Export to Excel** icon to export the data.

Monitoring LAN

The LAN menu includes the following submenus:

Monitoring Performance Information for Ethernet

To monitor the performance information for ethernet from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > LAN > Ethernet**.

The **Ethernet** window is displayed.

Step 2 You can use the drop-down to filter the view by Last 10 Minutes, Last Hour, Last Day, Last Week, Last Month, and Last Year.

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

- 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 export the data into a spreadsheet, click the **Export** icon in the upper-right corner and click **Save**.
- Use the chart icons to view the traffic chart in varied views. You can also use the icons to **Append**, **Predict**, and **Do not interpolate data**.

  Note Set the **pmchart.doInterpolate** property in the **Server Properties** window to false to use the **Do not interpolate data** option.

- For the Rx/Tx calculation, see the following Rx/Tx calculation.

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

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

Note If the performance tables do not contain any data, see the Thresholds section to turn on performance data collection.

Monitoring ISL Traffic and Errors

To monitor the ISL traffic and errors from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > LAN > Link**.

The **ISL Traffic and Errors** window is displayed. 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 Last 10 Minutes, Last Hour, Last Day, Last Week, Last Month, and Last Year.

Note **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 **Do not interpolate data**.

  Note Set the **pmchart.doInterpolate** property in the **Server Properties** window to false to use the **Do not interpolate data** option.

- To export the data into a spreadsheet, choose **Export** from the drop-down list in the **Chart** menu and then click **Save**.
- For the Rx/Tx calculation, see the following Rx/Tx calculation.

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

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

Note If the performance tables do not contain any data, see the Performance Setup Thresholds section to turn on performance.

Monitoring 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 endpoints. If there is an inconsistency in the vPC configurations, the vPC does not function correctly.



Note To view the vPC in **vPC Performance**, both primary and secondary device should be designated to the user. If either one kind of switch is not designated, vPC information is isplayed.

Cisco DCNM **Web Client** > **Monitor**> **vPC** displays only consistent vPCs displays both the consistent and inconsistent vPCs.

You can identify the inconsistent vPCs and resolve the inconsistencies in each vPC by using the Cisco DCNM **Web UI** > **Configure** > **Deploy** > **vPC Peer** and **Web Client** > **Configure** > **Deploy** > **vPC**.

Table 8: vPC Performance, on page 45 displays the following vPC configuration details in the data grid view.

Table 8: vPC Performance

Column	Description
Search box	Enter any string to filter the entries in their respective column.
vPC ID	Displays vPC ID's configured device.
Domain ID	Displays the domain ID of the vPC peer switches.
Multi Chassis vPC EndPoints	Displays the multi-chassis vPC endpoints for each vPC ID under a vPC domain.
Primary vPC Peer - Device Name	Displays the vPC Primary device name.
Primary vPC Peer - Primary vPC Interface	Displays the primary vPC interface.
Primary vPC Peer - Capacity	Displays the capacity for the primary vPC peer.
Primary vPC Peer - Avg. Rx/sec	Displays the average receiving speed of primary vPC peer.
Primary vPC Peer - Avg. Tx/sec	Displays the average sending speed of primary vPC peer.
Primary vPC Peer - Peak Util%	Displays the peak utilization percentage of primary vPC peer.
Secondary vPC Peer - Device Name	Displays the vPC secondary device name.
Secondary vPC Interface	Displays the secondary vPC interface.
Secondary vPC Peer - Capacity	Displays the capacity for the secondary vPC peer.
Secondary vPC Peer - Avg. Rx/sec	Displays the average receiving speed of secondary vPC peer.
Secondary vPC Peer - Avg. Tx/sec	Displays the average sending speed of secondary vPC peer.
Secondary vPC Peer - Peak Util%	Displays the peak utilization percentage of secondary vPC peer.

You can use this feature as following:

Monitoring vPC Performance

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

Note This tab only displays consistent vPCs.

To view the VPC performance information from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > LAN > vPC**.

The **vPC Performance** statistics is displayed. The aggregated statistics of all vPCs are displayed in a tabular manner.

Step 2 Click the **vPC ID**.

The vPC topology, **vPC Details**, **Peer-link Details**, and **Peer-link Status** are displayed.

The **vPC Consistency**, **Peer-link Consistency**, and **vPC Type2 Consistency** for the vPC are displayed.

- Click the **vPC Details** tab, you can view the parameter details of vPC **Basic Setting** and **Layer 2 Settings** for both Primary and Secondary vPC devices.
- Click the **Peer-link Details** tab, to view the parameter details of peer-link **vPC Global Setting** and **STP Global Settings** for both Primary and Secondary vPC devices.
- Click the **Peer-link Status** tab, the **vPC Consistency**, and **Peer-Link Consistency** status is displayed. The parameter details of **Role Status** and **vPC Peer keep-alive Status** for both Primary and Secondary vPC devices is also displayed.

Step 3 Click the peer-link icon in front of the **Device Name** in the **Primary vPC peer** or **Secondary vPC peer** column to view its member interface.

Step 4 Click the **Show 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 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 **Do not interpolate data**.

  Note Set the **pmchart.doInterpolate** property in the **Server Properties** window to false to use the **Do not interpolate data** option.

- To print the vPC Utilization data, click the **Print** icon in the upper-right corner. The vPC Utilization page appears.
- To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and click **Save File**.

Note If the performance tables do not contain any data, see the Thresholds section to turn on performance data collection.

Alarms

The Alarms menu includes the following submenus:

Viewing Alarms and Events

You can view the alarms, cleared alarms, and events.

Procedure

Step 1 Choose **Monitor** > **Alarms** > **View**.

Step 2 Choose any of the following tabs.

- **Alarms**: This tab displays the alarms that are generated for various categories. This tab displays information such as ID (optional), Severity, Failure Source, Name, Category, Acknowledged, Creation Time, Last Updated (optional), Policy, and Message. You can specify the **Refresh Interval** in this tab. You can select one or more alarms and then acknowledge or unacknowledge their status using the **Change Status** drop-down list. In addition, you can select one or more alarms and then click the **Delete** button to delete them.
- **Cleared Alarms**: This tab displays the cleared alarms. This tab displays information such as ID (optional), Severity, Failure Source, Name, Category, Acknowledged, Creation Time, Cleared At (optional), Cleared By, Policy, and Message. You can select one or more alarms and then click the **Delete** button to delete them.
- **Events**: This tab displays the events that are generated for the switches. This tab displays information such as **Ack**, **Acknowledged user**, **Group**, **Switch**, **Severity**, **Facility**, **Type**, **Count**, **Last Seen**, and **Description**. You can select one or more events and then acknowledge or unacknowledge their status using the **Change Status** drop-down list. In addition, you can select one or more alarms and then click the **Delete** button to delete them. If you want to delete all events, click the **Delete All** button.

Monitoring and Adding Alarm Policies



Note

- Alarm policies are stored in compute nodes. Therefore, run the **appmgr backup** command on each compute node in addition to taking a backup of DCNM.

You can add alarm policies for the following:

- **Device Health**: Device health policies enable you to create alarms when Device ICMP Unreachable, Device SNMP Unreachable, or Device SSH Unreachable. Also, these policies enable you to monitor chassis temperature, CPU, and memory usage.
- **Interface Health**: Interface health policies enable you to monitor Up or Down, Packet Discard, Error, Bandwidth details of the interfaces. By default all interfaces are selected for monitoring.
- **Syslog Alarm**: Syslog Alarm Policy defines a pair of Syslog messages formats; one which raises the alarm, and one which clears the alarm.

Procedure

Step 1 Choose **Monitor > Alarms > Alarm Policies**.

Step 2 Select the **Enable Alarms** check box to enable alarm policies.

Step 3 From the **Add** drop-down list, choose any of the following:

- Device Health Policy: Select the devices for which you want to create policies. Specify the policy name, description, CPU Utilization parameters, Memory Utilization parameters, Environment Temperature parameters, device availability, and device features. Under **Device Features**, you can select the BFD, BGP, and HSRP protocols. When these check boxes are selected, alarms are triggered for the following traps: **BFD**- ciscoBfdSessDown, ciscoBfdSessUp, **BGP**- bgpEstablishedNotification, bgpBackwardTransNotification, cbgpPeer2BackwardTransition (), cbgpPeer2EstablishedNotification, and **HSRP**- cHsrpStateChange. Please refer https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en for detailed trap OID definition.
- Interface Health Policy: Select the devices for which you want to create policies. Specify the policy name, description, link-state, Bandwidth (In/Out), Inbound errors, Outbound errors, Inbound Discards, and Outbound Discards.
- Syslog Alarm Policy: Select the devices for which you want to create policies and then specify the following parameters.
  - Devices: Define the scope of this policy. Select individual devices or all devices to apply this policy.
  - Policy Name: Specify the name for this policy. It must be unique.
  - Description: Specify a brief description for this policy.
  - Severity: Define the severity level for this syslog alarm policy. Choices are: Critical, Major, Minor, and Warning.
  - Identifier: Specify the identifier portions of the raise & clear messages.
  - Raise Regex: Define the format of a syslog raise message. The syntax is as follows: **Facility-Severity-Type: Message**
  - Clear Regex: Define the format of a syslog clear message. The syntax is as follows: **Facility-Severity-Type: Message**

Table 9: Example 1

Identifier	ID1-ID2
Raise Regex	ETHPORT-5-IF_ADMIN_UP: Interface Ethernet15/1 is admin up .
Clear Regex	ETHPORT-5-IF_DOWN_NONE: Interface Ethernet15/1 is down (Transceiver Absent)

In the above example, the regex expressions are part of the syslog messages that appear in the terminal monitor.

Table 10: Example 2

Identifier	ID1-ID2
Raise Regex	ETH_PORT_CHANNEL-5-PORT_DOWN: $(ID1): $(ID2) is down
Clear Regex	ETH_PORT_CHANNEL-5-PORT_UP: $(ID1): $(ID2) is up

Table 11: Example 3

Identifier	ID1-ID2
Raise Regex	ETHPORT-5-IF_SFP_WARNING: Interface $(ID1), High Rx Power Warning
Clear Regex	ETHPORT-5-IF_SFP_WARNING: Interface $(ID1), High Rx Power Warning cleared

Step 4 Click **OK** to add the policy.

Syslog Messages in Terminal Monitor and Console

The following examples show how the syslog messages appear in the terminal monitor and the console. The regex expression is matched with the part of the syslog messages after the % sign.

```
leaf-9516# terminal monitor
leaf-9516# conf t
leaf-9516(config)# int e15/1-32
leaf-9516(config-if-range)# no shut
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_ADMIN_UP: Interface
Ethernet15/1 is admin up .
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_DOWN_NONE: Interface
Ethernet15/1 is down (Transceiver Absent)
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_ADMIN_UP: Interface
Ethernet15/2 is admin up .
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_DOWN_NONE: Interface
Ethernet15/2 is down (Transceiver Absent)
2019 Aug 2 04:41:28 leaf-9516 %ETHPORT-5-IF_ADMIN_UP: Interface
Ethernet15/3 is admin up .
```

The syslog messages in the console have a similar format as they would appear in the terminal monitor, except for the additional port information enclosed in the %$ signs. However, the regex expression is matched with the part of the syslog messages after the last % sign.

```
SR-leaf1# 2019 Aug 26 23:55:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-
PFM_ALERT: FAN_BAD: fan6
2019 Aug 26 23:56:15 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:56:18 SR-leaf1 %$ VDC-1 %$ %ASCII-CFG-2-CONF_CONTROL:
System ready
2019 Aug 26 23:56:25 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:56:35 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
```

```
2019 Aug 26 23:56:39 SR-leaf1 %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE:
Successfully activated virtual service 'guestshell+'
2019 Aug 26 23:56:39 SR-leaf1 %$ VDC-1 %$ %VMAN-2-GUESTSHELL_ENABLED:
The guest shell has been enabled. The command 'guestshell' may be used
to access it, 'guestshell destroy' to remove it.
2019 Aug 26 23:56:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-2-FAN_REMOVED: Fan
module 5 (Serial number ) Fan5(sys_fan5) removed
2019 Aug 26 23:56:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
System will shutdown in 2 minutes 0 seconds due to fan policy
__pfm_fanabsent_any_singlefan.
2019 Aug 26 23:56:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:56:54 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
System will shutdown in 1 minutes 40 seconds due to fan policy
__pfm_fanabsent_any_singlefan.
2019 Aug 26 23:56:54 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:57:03 SR-leaf1 %$ VDC-1 %$ %PLATFORM-2-FANMOD_FAN_OK:
Fan module 5 (Fan5(sys_fan5) fan) ok
2019 Aug 26 23:57:03 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
```

Activating Policies

After you create new alarm policies, activate them.

Procedure

Step 1 Choose **Monitor > Alarms > Policies**.

Step 2 Select the policies that you want to activate and then click the **Activate** button.

Note Ensure that the port number for SNMP_TRAP is set to 2162, for DCNM to receive alarm traps.

Deactivating Policies

You can deactivate the active alarm policies.

Procedure

Step 1 Choose **Monitor > Alarms > Policies**.

Step 2 Select the policies that you want to deactivate and then click the **Deactivate** button.

Importing Policies

You can create alarm policies using the import functionality.

Procedure

Step 1 Choose **Monitor > Alarms > Policies** and then click the **Import** button.

Step 2 Browse and select the policy file saved on your computer.

You can only import policies in text format.

Exporting Policies

You can export the alarm policies into a text file.

Procedure

Step 1 From the menu bar, choose **Monitor > Alarms > Policies**.

Step 2 Click the **Export** button and then select a location on your computer to store the exported file.

Editing Policies

Procedure

Step 1 From the menu bar, choose **Monitor > Alarms > Policies**.

Step 2 Select the policy that you want to edit.

Step 3 Click the **Edit** button and then make necessary changes.

Step 4 Click the **OK** button.

Deleting Policies

Procedure

Step 1 From the menu bar, choose **Monitor > Alarms > Policies**.

Step 2 Select the policy that you want to delete.

Step 3 Click the **Delete** button. The policy is deleted.

Enabling External Alarms

You can enable external alarms using one of the following methods:

- Using Cisco DCNM Web UI

1. From Cisco DCNM Web UI, choose **Administration > DCNM Server > Server Properties**.
2. Locate the **alarm.enable.external** property.
3. Enter the value in the field as **true**.

- Using REST APIs
  1. Go the API documentation URL from your DCNM setup: https://<*DCNM-ip*>/api-docs
  2. Navigate to the **Alarms** section.
  3. Click **POST > rest/alarms/enabledisableextalarm**.
  4. Choose the **body** parameter value as **true** from the **Value** drop-down list.
  5. Click **Try it out!**.

- Using CLI
  1. Log into the DCNM server using SSH.
  2. Set the **alarm.enable.external** property to **true** in the server.properties file.

     The filepath is `/usr/local/cisco/dcm/fm/config/server.properties`.

Health Monitor Alarms

Starting from Cisco DCNM Release 11.4(1), alarms are registered and created under the External alarm category by the Health Monitor.

Health Monitor: Alarm Policy

The Health Monitor external alarm category policy is automatically activated and enabled on all the devices in a fabric. The severity level of this alarm policy can be MINOR, MAJOR, or CRITICAL.

Alarms are raised and categorized as CRITICAL for the following events:

- Elasticsearch (ES) Cluster Status is Red: Critical (For Cluster/HA mode only)
- CPU/Memory/Disk Utilization/ES JVM Heap Used Percentage >= 90%

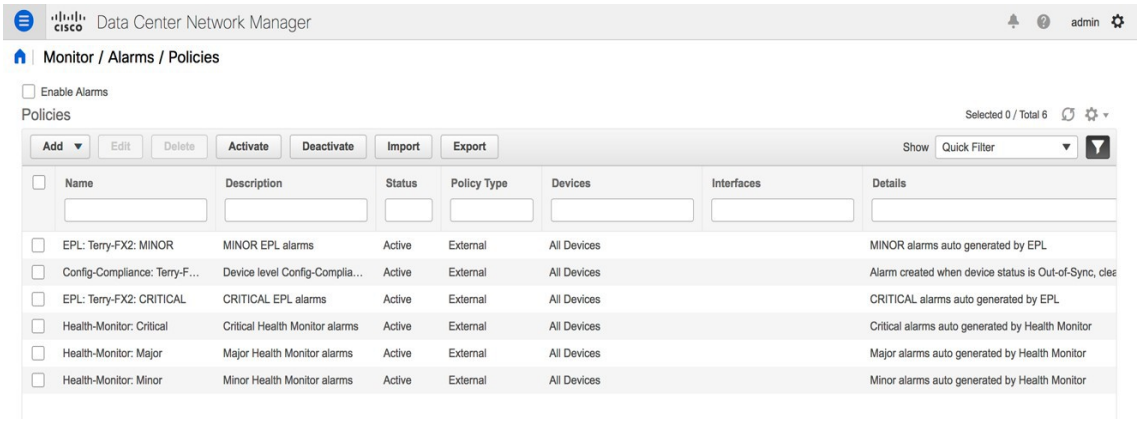
Alarms are raised and categorized as MAJOR for the following events:

- ES Cluster Status is Yellow (For Cluster/HA mode only)
- ES has unassigned shards (For Cluster/HA mode only)
- CPU/Memory/Disk Utilization/ES JVM Heap Used Percentage >= 80% and <90%

Alarms are raised and categorized as MINOR for the following events:

- CPU/Memory/Disk Utilization/ES JVM Heap Used Percentage >= 65% and <80%
- Kafka: Number of partitions without active leader > 0
- Kafka: Qualified partition leader not found. Unclear leaders > 0

Choose **Monitor>Alarms>Policies** to display the Health Monitor alarm policies. These alarm policies are not editable on the web UI. Click **Activate** or **Deactivate** to activate or deactivate the selected policy.



In case an alarm policy is deactivated using the GUI, any alarms created or cleared for that policy will not be displayed in the **Monitor>Alarms>View** tab. To delete a policy, select the checkbox next to the policy and click **Delete**. However, we recommend not deleting a policy from the GUI. When a fabric is deleted, the alarm policy along with all the active alarms for the devices in that fabric are deleted.

Health Monitor: Active Alarms

Choose **Monitor>Alarms>View** to display the active alarms.

To clear active alarms, select the checkbox next to the alarm, click **Change Status** and select **Clear**.

To delete active alarms, select the checkbox next to the alarm and click **Delete**.

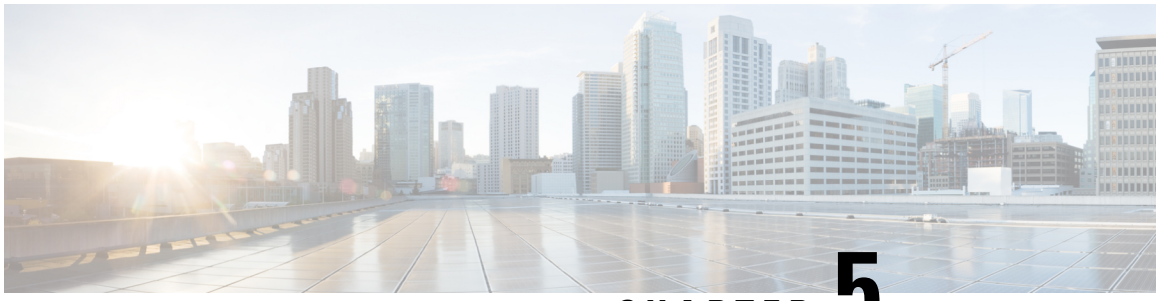
Health Monitor: Cleared Alarms

To view the cleared alarms, select **Monitor>Alarms>View>Cleared Alarms**.

Click the arrow icon ▶ to display detailed information about the required alarm.

To delete a cleared alarm from the list of cleared alarms, select the checkbox next to the alarm and click **Delete**.

For more information on Alarms and Policies, refer Alarms.



CHAPTER 5

Configure

This chapter contains the following topics:

- Deploy, on page 55
- Templates, on page 72
- Backup, on page 102
- Image Management, on page 114
- LAN Telemetry Health, on page 132

Deploy

The Deploy menu includes the following submenus:

POAP Launchpad

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

The POAP launchpad contains the following configuration steps:

Procedure

Step 1 Create and manage scopes for POAP creation.

Step 2 Set a server for images and configuration files.

Step 3 Generate from a template or upload existing configuration.

Power-On Auto Provisioning (POAP)

Power-On Auto Provisioning (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.

If the AAA authentication is set up before adding switch, "Invalid Credential" error appears during POAP. There is no functional impact. However, it refrains from DCNM receiving accurate POAP. You must update the `poap_dcnm.py file` located in **/var/lib/dcnm/** with the new AAA administrative password, by using the following command:

dcnm# **python poap_dcnm.py dcnm-info** *<dcnm-ipaddress> <username> <password>*

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.

If the POAP does not complete any configurations, you can refresh the configurations on the device. SSH to Cisco DCNM server and logon. Navigate to the DCNM directory by using the following command:

```
dcnm# cd /var/lib/dcnm/<switch_serial_number>
```

Locate the switch configuration file is the above directory. Refresh the configuration by using the following command:

```
dcnm# sed -i 's/\r//g' <config_file_for_switch>
```



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

DHCP Scopes

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 DCHP scope to distribute IPv4 address, PYTHON bootscript, (or other supported protocol + access credential + server) which stores the bootscript.

Choose **Configure > Deploy > POAP**.

The following table details the columns in the display.

Table 12: DCHP Scopes display fields

DHCP Scopes	Comment
Scope Name	The DHCP scope name must be unique among 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. Enter a valid IP as the default gateway.
Domain Name Servers	The domain name server for the DHCP scope.
Bootscript Name	The Python Bootup script.

DHCP Scopes	Comment
TFTP/Bootscript Server	The server that holds the bootscript.

Adding a DHCP Scope

To add a DHCP scope from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Deploy** > **POAP** > **DHCP Scopes**.

The **DCHP Scopes** window is displayed.

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 12: DCHP Scopes display fields, on page 56.

Step 4 Click **OK** to add a DHCP scope.

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.

To edit an existing DHCP scope from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Deploy** > **POAP** > **DHCP Scopes**.

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

To delete a DHCP scope from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Deploy** > **POAP** > **DHCP Scopes**.

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.

Image and Configuration Servers

The Image and Configuration Servers page allows you to specify the servers and credentials used to access the device images and the uploaded or Cisco DCNM generated or published device configuration. The server that is serving the images could be different from the one serving the configurations. If the same server is serving both images and configurations, you need to specify the server IP address and credentials twice for each server because the root directory holding the images or configuration files could be different. By default, the Cisco DCNM server will be the default image and configuration server. There will be two Cisco DCNM server addresses, one for configuration, one for image.

From the menu bar, choose **Configure > Deploy > POAP**. The Power-On Auto Provisioning (POAP) page appears. Click **Images and Configuration**.

The following table details the columns in the display.

Table 13: DCHP Scopes display fields

Image and Configuration Servers	Description
Name	Name of the image and configuration server.
URL	URL shows where images and files are stored.
Username	Indicates the username.
Last Modified	Indicates the last modified date.

You can add your own image and configuration servers if they are different from the default.

Add Image or Configuration Server URL

To add an image or a configuration server URL from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 On the Image and Configuration Servers page, click the **Add** icon.

Step 2 In the **Add Image or Configuration Servers URL** window, specify a name for the image.

Step 3 Select the **scp** radio button to select the SCP protocol for POAP and Image Management.

Step 4 Enter Hostname/Ipaddress and Path.

Step 5 Specify the Username and Password.

Step 6 Click **OK** to save.

Editing an Image or Configuration Server URL

To edit an image or a configuration server URL to the repository from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 On the Image and Configuration Servers page, select an existing Image and Configuration Server from the list, and click the **Edit** icon.

Step 2 In the **Edit Image or Configuration Servers URL** window, edit the required fields.

The Default_SCP_Repository cannot be edited.

Step 3 Click **OK** to save or click **Cancel** to discard the changes.

Deleting an Image or Configuration Server URL

To delete an image or a configuration server URL to the repository from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 On the Image and Configuration Servers page, select an existing Image and Configuration Server from the list, and click the **Delete** icon.

Step 2 In the delete notification, click **Yes** to delete the image and configuration server.

Note The default SCP Repository cannot be deleted.

Using the File Browser

The file browser feature enables you to browse through the repository.

To view the files using file browser from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 On the Image and Configuration Servers page, select an existing Image and Configuration Server from the list.

Step 2 Click the **File Browser** button to see the file in the directory. The File browser pop-up dialog appears.

Uploading an Image File

To upload an image file from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 On the **Image and Configuration Servers** window, select an existing **Image and Configuration Server** from the list.

Step 2 Click the **Image Upload** button.

Step 3 Click the **Choose File** button to choose an image file.

Step 4 In the **Platform** drop-down list, choose the hardware model name of the managed device. For example, N7K, N9K.

Step 5 In the **Type** drop-down list, choose the image type. For example, kickstart, system.

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, **Configure > Templates > Deploy**. 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

To add POAP templates from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Deploy > POAP > POAP Definitions**.

The **POAP Definitions** window is displayed.

Step 2 In the **Configuration Steps**, click the template hyperlink in the POAP Definitions section.

Step 3 Click the **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 template type from the drop-down list.

By default, CLI template type is selected.

Step 7 Select the **Published** checkbox if you want the template to have ‘Read Only’ access.

Step 8 In the **Template Content** pane, 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, on page 62 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

To edit a template from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Deploy** > **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 the **Modify or 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

To clone a template from an existing template, from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Deploy** > **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 **Save Template As** 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

To import a template from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Deploy** > **POAP**.

Step 2 Under **Configuration Steps**, click the template hyperlink in the **POAP Definitions** section.

Step 3 Select a template from the list and click **Import Template**.

Step 4 Select the template file and upload.

Exporting a Template

To export a template from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Deploy > 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.

To delete a template from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Deploy > 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 14: Annotation Keys

Key Name	Default Value	Description
DisplayName	Empty String	The value is displayed as a variable label in the template from GUI, on POAP definition screen.
Description	Empty String	Displays the description next or below the template variable field in the template from 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.
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 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 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.
Bootscript Status	Indicates the Bootscript execution state when the device executed POAP. For details, view the “Boot Log” file.

Fields and Icons	Description
Diff State	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 in sync with the POAP configuration. The different states are: • 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	Specifies the template used for creating the POAP definition. Fabric and IPFabric POAP templates are available.
Bootscript Last Updated Time	Specifies the last updated time for bootscript.
Last Published	Specifies the last published 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 POAP definition.
Icons	
Add	Allows you to add a POAP definition. For more information, see Creating a POAP Definition, on page 66.

Fields and Icons	Description
Edit	Allows you to edit a POAP definition. For more information, see Editing a POAP Definition, on page 68.
Delete	Allows you to delete a POAP definition. For more information, see Deleting POAP Definitions, on page 68.
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, on page 69.
Change Image	Allows you to change the image for the defined POAP definition. For more information, see Change Image, on page 69.
Boot Log	Display the list and view log files from the device bootflash.
Update Serial Number	Allows the user to modify the serial number of the POAP definition.
Refresh Switch	Refreshes the list of switches.
Refresh Diff State	Refreshes the Diff state.
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.

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

To create a POAP definition from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Deploy** > **POAP** > **POAP Definitions**.

Step 2 From the **Scope** drop-down list, select the scope for POAP definition.

Step 3 Click **Add** to add a new POAP definition.

Step 4 Click **Generate Definition** radio button to generate POAP definition from a template, and click **Next** to specify the switch details.

Step 5 Enter the serial number of switches that are separated by comma. Alternatively, you can click **Import from CSV File** to import the list of switches.

Note The serial number cannot be changed after you create the POAP definition. Verify that the serial numbers do not contain spaces, the POAP will not work otherwise.

Step 6 Use the drop-down list to select the Switch Type.

Step 7 Use the drop-down list to select the Image Server.

Step 8 Use the drop-down list to select the System Image and Kickstart image.

Step 9 Specify the Switch Username 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 From the **Settings File** drop-down list to select the file. If the settings file in unavailable, click **Save Parameter** as New Settings File button to specify a name for the settings file.

Step 14 Select the variables and click **Manage**.

Step 15 Click **Add** to see the variables to be saved.

Specify a name for the settings file and click **Save**.

Step 16 Click **Manage** to modify the settings file parameters.

Step 17 Click **Preview CLI** to view the generated configuration.

Step 18 Click **Finish** to publish the POAP definition.

Step 19 Click **Next** to generate the configuration.

Uploading a POAP Definition

To upload a POAP definition from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Deploy > POAP > POAP Definitions**.

Step 2 Click **Upload Startup Config** radio button to upload startup configuration 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 to select the System Image and Kickstart Image.

Step 7 Specify the Switch User Name and Password.

Step 8 Click **Browse** to select the upload configuration file.

Step 9 Click **Finish** to publish the POAP definition.

Editing a POAP Definition

To edit a POAP definition from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Deploy** > **POAP** > **POAP Definitions**.

Step 2 Select the POAP switch definitions from the list and click the **Edit** icon.

Step 3 Follow the steps listed in Creating a POAP Definition, on page 66 and Uploading a POAP Definition, on page 67 sections.

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

Deleting POAP Definitions

To delete POAP definitions from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Deploy** > **POAP** > **POAP Definitions**.

Step 2 Select the POAP switch definitions from the list and click **Delete** icon.

Step 3 Click **Yes** to delete the switch definitions.

A prompt appears to delete the device from the data source. Check or uncheck the checkbox based if you want to delete the switches associated with the POAP Definition.

Step 4 Click **OK** to confirm to delete the device. Based on the check box, the device will be deleted from the data source also.

Publishing POAP Definitions

Procedure

Step 1 Choose **Configure** > **Deploy** > **POAP** > **POAP Definitions**.

Step 2 Select the POAP switch definitions from the list and click **Publish**.

Step 3 Click **Yes** to publish the switch definitions.

Write, Erase, and Reload the POAP Switch Definition

To write, erase, and reload the POAP switch definition from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Deploy** > **POAP** > **POAP Definitions**.

Step 2 Select the POAP switch definitions from the list and click the **Edit** icon.

Step 3 Click **Write Erase and Reload**.

The **Write**, **Erase**, and **Reload** works only when the selected switches are listed in the **Inventory** > **Discovery** > **LAN Switches** window. Also, valid credentials must be specified in the **Configure** > **Credentials Management** > **LAN Credentials** window.

Step 4 Click **Continue** to reboot and reload the switch definitions.

Change Image

To change image from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Deploy** > **POAP** > **POAP Definitions**.

Step 2 Select the POAP switch definitions from the list and click the **Edit** icon.

Step 3 Select the switch for which you must 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** window is displayed.

Step 4 From the **Image Server** drop-down list, select the server where the new image is stored.

Step 5 From the **System Image** drop-down list, select the new system image.

Step 6 From the **Kickstart Image** drop-down list, select the new image which replaces the old image.

Step 7 Click **OK** to apply and change the image.

Updating the Serial Number of a Switch for an Existing POAP Definition

To update the serial number of a switch when performing an RMA from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Ensure that the old switch is in place with POAP definition and discovered.

Step 2 Manually update the serial number in Cisco DCNM on the POAP screen.

Note This button may be hidden underneath a >> button.

Now, two devices in Cisco DCNM have the same IP address.

Step 3 Physically remove the old switch from the network.

Step 4 Place the new switch in the rack and connect network cables and power. Bring up the new switch. The new switch reboots several times so that it comes up with necessary configurations.

Step 5 Manually rediscover the switches in Cisco DCNM.

There is one device in Cisco DCNM with the same IP address.

Cable Plan



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 that are 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.

The Cable plan configuration screen has the following options:

Create a Cable Plan

To create a cable plan from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Deploy** > **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) **Capture from existing deployment**: You can ascertain the Inter-Switch Links between existing switches that are managed by DCNM and "lock down" the cable plan based on the existing wiring.

b) **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

To view the existing cable plan deployment from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Deploy** > **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

To delete a cable plan from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Deploy** > **POAP** > **Cable Plan**.

Step 2 Click **Delete** icon.

Step 3 Click **Yes** to confirm deletion.

Deploying a Cable Plan

To deploy a cable plan from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Deploy** > **POAP** > **Cable Plan**.

Step 2 In the Switches table, use the checkbox to select the cable plan and click **Deploy a Cable Plan**.

Step 3 Click **Yes** to confirm deployment.

Revoking a Cable Plan

Procedure

Step 1 Choose **Configure** > **Deploy** > **POAP** > **Cable Plan**.

Step 2 In the Switches table, use the check box to select cable plans, and click **Revoke a Cable Plan**.

Step 3 Click **Yes** to confirm.

Viewing a Deployed Cable Plan from Device

To view the deployed cable plan from a device from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Deploy** > **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.

Templates

The **Templates** menu includes the following option:

Template Library

Template Library includes the following tabs:

Template Library

You can add, edit, or delete templates that are configured across different Cisco Nexus and Cisco MDS platforms using Cisco DCNM Web client. From Cisco DCNM Web client home page, choose **Configure** > **Templates** > **Template Library** > **Templates**. The following parameters are displayed for each template that is configured on Cisco DCNM Web client. Templates support JavaScript. You can use the JavaScript function in a template to perform arithmetic operations and string manipulations in the template syntax.

The following table describes the fields that appear on this page.

Table 15: Templates Operations

Field	Description
Add Template	Allows you to add a new template.
Launch job creation wizard	Allows you to create jobs.
Modify/View Template	Allows you to view the template definition and modify as required.
Save Template As	Allows you to save the selected template in a different name. You can edit the template as required.
Delete Template	Allows you to delete a template
Import Template	Allows you to import a template from your local directory, one at a time.
Export template	Allows you to export the template configuration to a local directory location.
Import Template Zip File	Allows you to import `.zip` file, that contains more than one template that is bundled in a `.zip` format All the templates in the ZIP file are extracted and listed in the table as individual templates.

Note Notifications appear next to **Import Template Zip File** if there are issues while loading templates after restarting the server. Click the notifications to see the errors in the **Issues in loading Template** window. Templates with errors are not listed in the **Templates** window. To import these templates, correct the errors, and import them.

Table 16: Template Properties

Field	Description
Template Name	Displays the name of the configured template.
Template Description	Displays the description that is provided while configuring templates.
Tags	Displays the tag that is assigned for the template and aids to filter templates based on the tags.
Supported Platforms	Displays the supported Cisco Nexus platforms compatible with the template. Check the check box of platforms that are supported with the template. **Note** You can select multiple platforms.
Template Type	Displays the type of the template.
Template Sub Type	Specifies the sub type that is associated with the template.
Template Content Type	Specifies if it is Jython or Template CLI.

Table 17: Advanced Template Properties

Field	Description
Implements	Displays the abstract template to be implemented.
Dependencies	Specifies the specific feature of a switch.
Published	Specifies if the template is published or not.
Imports	Specifies the base template for importing.

In addition, from the menu bar, choose **Configure** > **Templates** > **Template Library** > **Templates** and you can also:

- Click **Show Filter** to filter the templates that is based on the headers.
- Click **Print** to print the list of templates.
- Click **Export to Excel** to export the list of template to a Microsoft Excel spreadsheet.

This section contains the following:

Template Structure

The configuration template content mainly consists of four parts. Click the **Help** icon next to the **Template Content** for information about editing the content of the template.

This section contains the following:

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 configuration template. Specify ‘All’ to support all platforms.	N1K, N3K, N3500, N4K, N5K, N5500, N5600, N6K, N7K, N9K, MDS, VDC, N9K-9000v, IOS-XE, IOS-XR, Others, All Nexus Switches list separated by comma.	No
templateType	Specifies the type of Template used.	• CLI • POAP • POLICY • SHOW • PROFILE • FABRIC • ABSTRACT	Yes

Property Name	Description	Valid Values	Optional?
templateSubType	Specifies the sub type associated with the template.		

Property Name	Description	Valid Values	Optional?
		• CLI • N/A • POAP • N/A • VXLAN • FABRICPATH • VLAN • PMN • POLICY • VLAN • INTERFACE_VLAN • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORT_CHANNEL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VFC • INTERFACE_SAN_PORT_CHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE • SHOW • VLAN • INTERFACE_VLAN • INTERFACE_VPC	

Property Name	Description	Valid Values	Optional?
		• INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORT_CHANNEL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VFC • INTERFACE_SUBINTERFACE • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE • PROFILE • VXLAN • FABRIC • NA	

Property Name	Description	Valid Values	Optional?
		• ABSTRACT • VLAN • INTERFACE_VLAN • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORT_CHANNEL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VFC • INTERFACE_SAN_PORT_CHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE	

Property Name	Description	Valid Values	Optional?
contentType		• CLI • TEMPLATE_CLI • POAP • TEMPLATE_CLI • POLICY • TEMPLATE_CLI • PYTHON • SHOW • TEMPLATE_CLI • PROFILE • TEMPLATE_CLI • PYTHON • FABRIC • PYTHON • ABSTRACT • TEMPLATE_CLI • PYTHON	Yes
implements	Used to implement the abstract template.	Text	Yes
dependencies	Used to select the specific feature of a switch.	Text	Yes
published	Used to Mark the template as read only and avoids changes to it.	“true” or “false”	Yes

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?
boolean	true|false	No
enum	Example: running-config, startup-config	No
float	Floating number format	No
floatRange	Example: 10.1,50.01	Yes
Integer	Any number	No
integerRange	Contiguous numbers separated by "-" Discrete numbers separated by "," Example: 1-10,15,18,20	Yes
interface	Format: <if type><slot>[/<sub slot>]/<port> Example: eth1/1, fa10/1/2 etc.	No
interfaceRange	Example: eth10/1/20-25, eth11/1-5	Yes
ipAddress	IPv4 OR IPv6 address	No
ipAddressList	You can have a list of IPv4, IPv6, or a combination of both types of addresses. Example 1: 172.22.31.97, 172.22.31.99, 172.22.31.105, 172.22.31.109 Example 2: 2001:0db8:85a3:0000:0000:8a2e:0370:7334, 2001:0db8:85a3:0000:0000:8a2e:0370:7335, 2001:0db8:85a3:1230:0000:8a2f:0370:7334 Example 3: 172.22.31.97, 172.22.31.99, 2001:0db8:85a3:0000:0000:8a2e:0370:7334, 172.22.31.254	Yes

Variable Type	Valid Value	Iterative?

ipAddressWithoutPrefix	`Example: 192.168.1.1`
	or
	`Example: 1:2:3:4:5:6:7:8`
		No

ipV4Address	IPv4 address	No
ipV4AddressWithSubnet	`Example: 192.168.1.1/24`	No
ipV6Address	IPv6 address	No
ipV6AddressWithPrefix	`Example: 1:2:3:4:5:6:7:8` `22`	No
ipV6AddressWithSubnet	IPv6 Address with Subnet	No
ISISNetAddress	`Example:` `49.0001.00a0.c96b.c490.00`	No
long	`Example: 100`	No
macAddress	14 or 17 character length MAC address format	No

string	Free text, for example, used for the description of a variable
	`Example:`
	`string scheduledTime`
	`{`
	`regularExpr=^([01]\d|2[0-3]):([0-5]\d)$;`
	`}`
		No

string[]	`Example: {a,b,c,str1,str2}`	Yes

Variable Type	Valid Value	Iterative?

struct	Set of parameters that are bundled under a single variable.
	
	`struct <structure name declaration > {`
	`<parameter type> <parameter 1>;`
	`<parameter type> <parameter 2>;`
	`…..`
	`} [<structure_inst1>] [, <structure_inst2>] [, <structure_array_inst3 []>];`
	
	`struct interface_detail {`
	`string inf_name;`
	`string inf_description;`
	`ipAddress inf_host;`
	`enum duplex {`
	`validValues = auto, full, half;`
	`};`
	`}myInterface, myInterfaceArray[];`
		No
		
		Note If the struct variable is declared as an array, the variable is iterative.

wwn (Available only in Cisco DCNM Web Client)	`Example: 20:01:00:08:02:11:05:03`	No

Variable Meta Property

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

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

Variable Type	Description	Variable Meta Property											
		default Value	valid Values	decimal Length	min	max	min Slot	max Slot	min Port	max Port	min Length	max Length	regular Expr
boolean	A boolean value. `Example: true`	Yes											
enum			Yes										

Variable Type	Description	Variable Meta Property											
		default Value	valid Values	decimal Length	min	max	min Slot	max Slot	min Port	max Port	min Length	max Length	regular Expr
float	signed real number. Example: 75.56, -8.5	Yes	Yes	Yes	Yes	Yes							
floatRange	range of signed real numbers Example: 50.5 - 54.75	Yes	Yes	Yes	Yes	Yes							
integer	signed number Example: 50, -75	Yes	Yes		Yes	Yes							
integerRange	Range of signed numbers Example: 50-65	Yes	Yes		Yes	Yes							
interface	specifies interface/port Example: Ethernet 5/10	Yes	Yes				Yes	Yes	Yes	Yes			
interfaceRange		Yes	Yes				Yes	Yes	Yes	Yes			
ipAddress	IP address in IPv4 or IPv6 format	Yes											

Variable Type	Description	Variable Meta Property											
		default Value	valid Values	decimal Length	min	max	min Slot	max Slot	min Port	max Port	min Length	max Length	regular Expr
ipAddrList	You can have a list of IPv4, IPv6, or a combination of both types of addresses. Example 1: 172.22.31.97, 172.22.31.99, 172.22.31.105, 172.22.31.109 Example 2: [redacted] Example 3: 172.22.31.97, 172.22.31.99, [redacted], 172.22.31.254 **Note** Separate the addresses in the list using commas and not hyphens.	Yes											

Variable Type	Description	Variable Meta Property											
		default Value	valid Values	decimal Length	min	max	min Slot	max Slot	min Port	max Port	min Length	max Length	regular Expr
ipAddress	IPv4 or IPv6 Address (does not require prefix/subnet)												
ipV4Address	IPv4 address	Yes											
ipV4AddressWithSubnet	IPv4 Address with Subnet	Yes											
ipV6Address	IPv6 address	Yes											
ipV6AddressWithPrefix	IPv6 Address with prefix	Yes											
ipV6AddressWithSubnet	IPv6 Address with Subnet	Yes											
ISNAddress	Example: 4085554270												
long	Example: 100	Yes			Yes	Yes							
macAddress	MAC address												

Variable Type	Description	Variable Meta Property											
		default Value	valid Values	decimal Length	min	max	min Slot	max Slot	min Port	max Port	min Length	max Length	regular Expr
string	literal string Example for string Regular expression: string schedule { }	Yes									Yes	Yes	Yes
string[]	string literals that are separated by a comma (,) Example: {string1, string2}	Yes											

Variable Type	Description	Variable Meta Property											
		default Value	valid Values	decimal Length	min	max	min Slot	max Slot	min Port	max Port	min Length	max Length	regular Expr
struct	Set of parameters that are bundled under a single variable. `struct <structure name declaration > { <parameter type> <parameter 1>; <parameter type> <parameter 2>; ….. } [structureInstance1] [, <structureInstance2> [, <structureInstance3> []>];`												
wwn	WWN address												

Example: Meta Property Usage

```
##template variables

integer VLAN_ID {
min = 100;
max= 200;
};

string USER_NAME {
defaultValue = admin123;
minLength = 5;
};

struct interface_a{
```

```
 string inf_name;
 string inf_description;
 ipAddress inf_host;
 enum duplex {
  validValues = auto, full, half;
 };
}myInterface;

##
```

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	Description
AutoPopulate	Text	Copies values from one field to another
DataDepend	Text	
Description	Text	Description of the field appearing in the window
DisplayName	Text **Note** Enclose the text with quotes, if there is space.	Display name of the field appearing in the window
Enum	Text1, Text2, Text3, and so on	Lists the text or numeric values to select from
IsAlphaNumeric	"true" or "false"	Validates if the string is alphanumeric
IsAsn	"true" or "false"	
IsDestinationDevice	"true" or "false"	
IsDestinationFabric	"true" or "false"	
IsDestinationInterface	"true" or "false"	
IsDestinationSwitchName	"true" or "false"	
IsDeviceID	"true" or "false"	
IsDot1qId	"true" or "false"	

Annotation Key	Valid Values	Description
IsFEXID	“true” or “false”	
IsGateway	“true” or “false”	Validates if the IP address is a gateway
IsInternal	“true” or “false”	Makes the fields internal and does not display them on the window **Note** Use this annotation only for the ipAddress variable.
IsManagementIP	“true” or “false” **Note** This annotation must be marked only for variable “ipAddress”.	
IsMandatory	“true” or “false”	Validates if a value should be passed to the field mandatorily
IsMTU	“true” or “false”	
IsMultiCastGroupAddress	“true” or “false”	
IsMultiLineString	“true” or “false”	Converts a string field to multiline string text area
IsMultiplicity	“true” or “false”	
IsPassword	“true” or “false”	
IsPositive	“true” or “false”	Checks if the value is positive
IsReplicationMode	“true” or “false”	
IsShow	“true” or “false”	Displays or hides a field on the window
IsSiteId	“true” or “false”	
IsSourceDevice	“true” or “false”	
IsSourceFabric	“true” or “false”	
IsSourceInterface	“true” or “false”	

Annotation Key	Valid Values	Description
IsSourceSwitchName	“true” or “false”	
IsSwitchName	“true” or “false”	
IsRMID	“true” or “false”	
IsVPCDomainID	“true” or “false”	
IsVPCID	“true” or “false”	
IsVPCPeerLinkPort	“true” or “false”	
IsVPCPeerLinkPortChannel	“true” or “false”	
IsVPCPortChannel	“true” or “false”	
Password	Text	Validates the password field
UsePool	“true” or “false”	
UseDNSReverseLookup		
Username	Text	Displays the username field on the window
Warning	Text	Provides text to override the Description annotation

Example: AutoPopulate Annotation

```
##template variables
string BGP_AS;
 @(AutoPopulate="BGP_AS")
  string SITE_ID;
##
```

Example: DisplayName Annotation

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

Example: IsMandatory Annotation

```
##template variables
@(IsMandatory="ipv6!=null")
ipV4Address ipv4;
@(IsMandatory="ipv4!=null")
ipV6Address ipv6;
##
```

Example: IsMultiLineString Annotation

```
##template variables
@(IsMultiLineString=true)
string EXTRA_CONF_SPINE;
##
```

IsShow Annotation

```
##template variables
boolean isVlan;
@(IsShow="isVlan==true")
integer vlanNo;
##

##template variables
boolean enableScheduledBackup;
@(IsShow="enableScheduledBackup==true",Description="Server time")
string scheduledTime;
##
The condition "enableScheduledBackup==true" evaluates to true/false

##template variables
@(Enum="Manual,Back2BackOnly,ToExternalOnly,Both")
string VRF_LITE_AUTOCONFIG;
@(IsShow="VRF_LITE_AUTOCONFIG!=Manual",  Description="Target Mask")
integer DCI_SUBNET_TARGET_MASK
##
The condition "VRF_LITE_AUTOCONFIG!=Manual" matches string comparison to evaluate to true
or false
```

Example: Warning Annotation

```
##template variables
@(Warning="This is a warning msg")
  string SITE_ID;
##
```

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, you can 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]**

Template Content Editor

The template content editor has the following features:

- Syntax highlighting: The editor highlights the syntax, like different types of statements, keywords, and so on, for Python scripting.
- Autocompletion: The editor suggests the template datatypes, annotations, or metaproperties when you start typing.
- Go to line: You can navigate to the exact line in the template content editor instead of scrolling. Press **Command-L** in Mac or **Ctrl-L** in Windows, and enter the line number to which you want to navigate to in the pop-up window.

  If you enter a value greater than the number of lines in the editor, you will be navigated to the last line in the editor window.

- Template search and replace: Press **Command-F** in Mac or **Ctrl-F** in Windows, enter the search term in the **Search for** field, and select the type of search in the search window. You can perform the following searches in the editor:
  - **RegExp Search**: You can perform the regular expression search in the editor.
  - **CaseSensitive Search**: You can perform a case-sensitive search in the editor.
  - **Whole Word Search**: You can perform a whole word search to find the exact words in the editor. For example, a regular search for the word "play" returns results where it is part of words like "display," but the whole word search returns results only when there is an exact match for the word "play".
  - **Search In Selection**: You can perform a search in the selected content. Select the content to which you want to limit the search and enter the search term.

  Choose the + icon in the search window to use the replace option. Enter the replacing word in the **Replace with** field. You can replace the selected word once by selecting **Replace**. To replace all the occurrences of the selected word, select **All**.

- Code folding: You can expand or group code blocks in the editor by clicking the arrow next to their line numbers.

- Other features: The editor automatically indents the code, the closing braces, and highlights the matching parenthesis.

Template Editor Settings

You can edit the following features of a template editor by clicking **Template Editor Settings**.

- **Theme**: Select the required theme for the editor from the drop-down list.
- **KeyBinding**: Select the editor mode from the **KeyBinding** drop-down list to customize the editor. **Vim** and **Ace** modes are supported. The default is **Ace**.
- **Font Size**: Select the required font size for the editor.

Advanced Features

The following are the advanced features available to configure templates.

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

  If a statement does not follow these guidelines, or if it does not suit this format, it will 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 that is located at the backend of the Java script file.

- Dynamic decision

  Config template 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 that are based on the device condition.

  Note The if block must be followed by an else block in a new line, which can be empty.

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

  ```
  Example: Create VLAN
  ##template content
  show vlan id $$vlan_id$$
  if($$LAST_CMD_RESPONSE$$ contains "not found"){
  vlan $$vlan_id$$
  }
  else{
  }
  ##
  ```

  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. In addition, the substituted content is used for complete CLI command generation.

- Solution POAP Templates for VXLAN and FabricPath

  From Cisco DCNM Release 10.0(1), Cisco provides you a set of defined templates to aid in POAP operations. You can download Cisco-defined templates from https://software.cisco.com/download/release.html.

  For instructions on how to download and install POAP templates, see *Cisco DCNM Installation Guide, Release 10.0(x)*.

Adding a Template

To add user-defined templates and schedule jobs from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Templates > Template Library > Templates**.

The **Templates** window is displayed with the name of the template along with its description, supported platforms, and tags.

Step 2 Click **Add** to add a new template.

The Template Properties window appears.

Step 3 Specify a template name, description, tags, and supported platforms for the new template.

Step 4 Specify a **Template Type** for the template. Select **POAP** to make this template available when you power on the application.

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

Step 5 Select a **Template Sub Type** and **Template Content Type** for the template.

Step 6 Click the **Advanced** tab to edit other properties like **Implements**, **Dependencies**, **Published**, and **Imports**. Select **Published** to make the template read-only. You cannot edit a published template.

Step 7 From the **Imports > Template Name** list, check the template check box.

The base template content is displayed in the **Template Content** window. The base template displays the template properties, template variables, and template content. This template can be imported in to another template and the base template content is substituted in the appropriate place of the extending template. When you launch the extended template, the parameter inputs for the base template are also obtained. Also, the substituted content is used for complete CLI command generation.

Note The base templates are CLI templates.

Step 8 Click **OK** to save the template properties, or click the cancel icon at the top-right corner of the window to revert the changes.

Note You can edit the template properties by clicking **Template Property**.

Step 9 Click **Template Content** to edit the template syntax. For information about the structure of the Configuration Template, see the *Template Structure* section.

Step 10 Click **Validate Template Syntax** to validate the template values.

If an error or a warning message appears, you can check the validation details in **Validation Table** by clicking the error and warnings field.

Note You can continue to save the template if there are warnings only. However, if there is an error, you must edit the templates to fix the errors before you proceed. Click the line number under the Start Line column to locate the error in the template content. You will get an error if you validate a template that does not have a template name.

Step 11 Click **Save** to save the template.

Step 12 Click **Save and Exit** to save the configuration and go back to the configuring templates screen.

Configuring Template Job

To configure and schedule jobs for individual templates from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Templates > Template Library > Templates**.

Step 2 Select a template.

Note Config Job wizard is applicable only for CLI templates.

Step 3 Click **Launch job creation wizard** icon and click **Next**.

Step 4 Use the drop-down to select **Device Scope**.

The devices that are configured under the selected **Device Scope** are displayed.

Note If no devices are displayed, check if the device LAN credentials are configured by choosing **Administration > Credentials Management > LAN Credentials**.

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

Step 6 In the **Define Variable** section, specify the VSAN_ID, VLAN_ID, ETH_SLOT_NUMBER, VFC_SLOT_NUMBER, SWITCH_PORT_MODE, ETH_PORT_RANGE and ALLOWED_VLANS values.

Note Based on the selected template, variables vary.

Step 7 In the **Edit Variable Per Device** section, double click the fields 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 name and description.

The Device Credentials are populated from **Administration > Credentials Management > LAN Credentials**.

Step 10 Use the radio button to select **Instant Job** or **Schedule Job**.

If you select **Schedule Job**, specify the date and time for the job delivery.

Step 11 Use the check box to select **Copy Run to Start**.

Step 12 If you want to configure more transaction and delivery options, use the check box to select **Show more options**.

Step 13 Under **Transaction Options(Optional)**, if you have a device with rollback feature support, select **Enable Rollback** check box and select the appropriate radio button.

You can choose one of the following options by selecting the appropriate radio button:

- **Rollback the configuration on a device if there is any failure on that device**
- **Rollback the configuration on all the devices if there is any failure on any device**
- **Rollback the configuration on a device if there is any failure on any device and stop further configuration delivery to remaining devices**

Step 14 Under **Delivery Options (Optional)**, specify the command response timeout in seconds and use the radio button to select a delivery order. The value of command response timeout ranges from 1 to 180.

You can choose one of the following options by selecting the appropriate radio button:

- **Deliver configuration one device at a time in sequential**
- **Delivery configuration in parallel to all devices at the same time**

Step 15 Click **Finish** to create the job.

A confirmation message is displayed that the job has been successfully created. The jobs are listed in the **Jobs** window.

Modifying a Template

You can edit the user-defined templates. However, the predefined templates and templates that are already published cannot be edited.

Procedure

Step 1 From **Configure > Templates > Template Library > Templates**, select a template.

Step 2 Click **Modify/View template**.

Step 3 Edit the template description and tags.

The edited template content is displayed in a pane on the right.

Step 4 From the **Imports > Template Name** list, check the template check box.

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 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.

Copying a Template

To copy a template from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Templates > Template Library > Templates**, and select a template.

Step 2 Click **Save Template As**.

Step 3 Edit the template name, description, tags, and other parameters.

The edited template content is displayed in the right-hand pane.

Step 4 From the **Imports > Template Name** list, check the template check box.

The base template content is displayed in the **Template Content** window. You can edit the template content that is based on your requirement in the **Template Content** window. Click 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.

Deleting a Template

You can delete the user-defined templates. However, you cannot delete the predefined templates. From Cisco DCNM Release 11.0(1), you can delete multiple templates at once.

To delete a template from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Templates** > **Template Library** > **Templates**.

Step 2 Use the check box to select a template and click **Remove template** icon.

The template is deleted without any warning message.

What to do next

The template is deleted from the list of templates on the DCNM Web UI. When you restart the DCNM services, the deleted templates are displayed on the **Configure** > **Templates** > **Template Library** > **Templates** page.

To delete the template permanently, delete the template that is located in your local directory: `Cisco Systems\dcm\dcnm\data\templates\`.

Importing a Template

To import a template from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Templates** > **Template Library** > **Templates** and click **Import Template**.

Step 2 Browse and select the template that is saved on your computer.

You can edit the template parameters, if necessary. For information, see Modifying a Template, on page 98.

Note The "\n" in the template is considered as a new line character when imported and edited, but it works fine when imported as a ZIP file.

Step 3 Click **Validate Template Syntax** to validate the template.

Step 4 Click **Save** to save the template or **Save and Exit** to save the template and exit.

Note You can import Cisco-defined FabricPath and IP VXLAN Programmable Fabric POAP Templates to the Cisco DCNM Web Client. For more information, see *Installing POAP Templates*.

Exporting a Template

To export a template from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Templates** > **Template Library** > **Templates**.

Step 2 Use the check box to select a template and click **Export Template**.

The browser requests you to open or save the template to your directory.

Installing POAP Templates

Cisco DCNM allows you to add, edit, or delete user-defined templates that are configured across different Cisco Nexus platforms. From Cisco DCNM Release 10.0(x), Cisco-defined FabricPath and IP VXLAN Programmable Fabric POAP Templates are provided as a separate download on the official Cisco website. These templates are compatible for use with the DCNM Virtual Appliance (OVA or ISO) for use with Nexus 2000, Nexus 5000, Nexus 6000, Nexus 7000, and Nexus 9000 Series switches.

You can download the Cisco-defined templates from https://software.cisco.com/download/release.html.

Perform the following task to install the POAP templates from the Cisco DCNM.

Procedure

Step 1 Navigate to https://software.cisco.com/download/release.html, and download the file.

You can choose one of the following:

- `dcnm_ip_vxlan_fabric_templates.10.0.1a.zip`
- `dcnm_fabricpath_fabric_templates.10.0.1a.zip file`

Step 2 Unzip and extract the files to the local directory on your computer.

Step 3 Choose **Configure** > **Templates** > **Template Library** > **Templates**.

Step 4 Click **Import Template**.

Step 5 Browse and select the template that is saved on your computer. You can edit the template parameters, if necessary.

Step 6 Check **POAP** and **Publish** check box to designate these templates as POAP templates.

Step 7 Click **Validate Template Syntax** to validate the template.

Step 8 Click **Save** to save the template or **Save and Exit** to save the template and exit.

Configuring Jobs

To configure jobs from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Templates** > **Templates Library** > **Jobs**.

The jobs are listed along with the Job ID, description and status. The latest task will be listed at the top.

Note If failover is triggered in Native HA, the Job ID sequence number is incremented by 32.

Step 2 Click **Show Filter** to filter the list.

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.

Step 4 To view the status of a job, click the **Job ID** radio button and click **Status**.

Step 5 To view the command execution status for a device, click the radio button of a device name from the **Devices** table in the **Job Execution Status** window.

Note You can delete multiple jobs at once, but you cannot view the status of multiple jobs at once.

Backup

The **Backup** menu includes the following submenus:

Switch Configuration

This feature allows you to backup device configurations from running configuration as a regular text file in the file system. However, you can also perform operations on startup configuration. The backup files can be stored in the DCNM server host or on a file server.

You can also configure the archive system to support scheduling of jobs for the selected list of devices. You can configure only one job for a switch.

The following tables describe the icons and fields that appear on **Configure > Backup > Switch Configuration**.

Table 18: Switch Configuration Operations

Icon	Description
Copy Configuration to bootflash	Allows you to copy a configuration file of a switch to the bootflash of the selected destination switches.
View Configuration	Allows you to view the configuration file.
Delete Configuration	Allows you to delete the configuration file.
Compare Configuration	Allows you to compare two configuration files, from different devices or on the same device.
Export Configuration	Allows you to export a configuration file from the DCNM server.
Import User-Defined Configuration	Allows you to import a user-defined configuration file to the DCNM server.
Restore Configuration to devices	Allows you to restore configuration from the selected devices.
Archive Jobs	Allows you to add, delete, view, or modify the jobs.

Table 19: Switch Configuration Field and Description

Field	Description
Device Name	Displays the device name Click the arrow next to the device to view the configuration files.
IP Address	Displays the IP address of the device.
Group	Displays the group of the device.
Configuration	Displays the configuration files that are archived for that device.
Archive Time	Displays the time when the device configuration files were archived. The format is Day:Mon:DD:YYYY HH:MM:SS.
Size	Displays the size of the archived file.

This section contains the following:

Copy Configuration

You can copy the configuration files to the same device, to another device, or multiple devices concurrently.

Perform the following task to view the status of tasks.

Procedure

Step 1 From Cisco DCNM home page, choose **Configure > Backup > Switch Configuration**. Select any startup/running/archive configuration of the device that you must copy.

Step 2 Click **Copy Configuration to bootflash**.

Copy Configuration to bootflash page appears, displaying the **Source Configuration Preview** and **Selected Devices** area.

Source Configuration Preview area shows the contents of running/startup/version configuration file which is copied to the devices.

Step 3 In the **Selected Devices** area, check the device name check box to copy the configuration to the device.

Note You can select multiple destination devices to copy the configuration.

The selected devices area shows the following fields:

- Device Name—Specifies the target device name to which the source configuration is copied.
- IP Address—Specifies the IP Address of the destination device.
- Group—Specifies the group to which the device belongs.
- Status—Specifies the status of the device.

Step 4 Click **Copy**.

A confirmation window appears.

Step 5 Click **Yes** to copy the configuration to the destination device configuration.

View Configuration

You can view or edit the configuration file on the device.

Perform the following task to view or edit the configuration file for the devices.

Procedure

Step 1 From Cisco DCNM home page, choose **Configure > Backup > Switch Configuration**. Click the arrow next to the device name to view the configuration files on the device. Select the configuration file radio button to view the configuration file.

Step 2 Click the View Configuration.

The View Configuration window appears showing the configuration file content.

Delete Configuration

Perform the following task to delete the configuration file from the device.

Note Ensure that you take a backup of the configuration file before you delete.

Procedure

Step 1 From Cisco DCNM home page, choose **Configure > Backup > Switch Configuration**. Click the arrow next to the device name to view the configuration files on the device.

Step 2 Click the configuration file radio button to be deleted.

Note You can delete multiple configuration files. However, you cannot delete startup, or running configuration files.

Step 3 Click **Yes** to delete the configuration file.

Compare Configuration Files

This feature allows you to compare the configuration file with another version of the same device or with the configuration file of another device.

Perform the following task to compare the configuration files.

Procedure

Step 1 Navigate to **Configure > Backup > Switch Configuration**. Click the arrow next to the device name to view the configuration files on the device.

Step 2 Check the check box and select two configuration files to compare.

The first file that you selected is designated as Source and the second configuration file is designated as the Target file.

Step 3 Click **Compare Configuration**.

View Config Diff page appears, displaying the difference between the two configuration files.

The Source and Target configuration files content is displayed in two columns. From the drop-down list in the right-top corner, choose **All** to view the entire configuration. You can also choose **Changed** to view the configuration differences of the configuration files.

The differences in the configuration file are show in the table, with legends.

- **Red**: Deleted configuration details.
- **Green**: New added configuration.
- **Blue**: Modified configuration details.

Step 4 Click **Copy to Target** to copy the source configuration to the target configuration file. Click **Cancel** to revert to the configuration details page.

The Copy Configuration window displays the source configuration preview and the target device of the destination configuration. The selected devices area shows the following fields:

- Device Name—Specifies the target device name to which the source configuration is copied.
- IP Address—Specifies the IP Address of the destination device.
- Group—Specifies the group to which the device belongs.
- Status—Specifies the status of the device.

Step 5 Click **Yes** to copy the configuration to the destination device configuration.

Export Configuration

You can export a configuration file from the Cisco DCNM server. Perform the following task to export a configuration file.

Procedure

Step 1 From Cisco DCNM home page, choose **Configure > Backup**, select a configuration to export.

Step 2 Click **Export Configuration**.

The files are downloaded in your local system. You can use the third-party file transfer tools to transfer these files to an external server.

Import Configuration File

You can import the configuration file from the file server to the Cisco DCNM.

Perform the following task to import a single or multiple configuration files.

Procedure

Step 1 From Cisco DCNM home page, choose **Configure > Backup > Switch Configuration** and click **Import User-Defined Configuration**.

The file server directory opens.

Step 2 Browse the directory and select the configuration file that you want to import. Click **Open**.

A confirmation screen appears.

Note The file name should not contain forward slash (/) or backward slash (\).

Step 3 Click **Yes** to import the selected file.

The imported configuration file appears as a User Imported file.

Restore Configuration

You can restore the configuration file from the selected switches. From Cisco DCNM Release 11.0(1), you can restore configuration based on the selected date as well.



Note You cannot restore the configuration for SAN switches and FCoE-enabled switches.

Perform the following task to restore the configuration from the selected devices.

Procedure

Step 1 From Cisco DCNM home page, choose **Configure > Backup > Switch Configuration**, and click **Restore**.

Step 2 Select the type of restore from the drop-down list. You can choose **Version-based** or **Date-based**.

Note
- If you choose date-based restore, you have to select the date and time. The configuration available before the mentioned time is restored.
- If you choose version-based restore, you have to choose a configuration from the **Configuration** column. You can view the configuration details in the **View** column.

Step 3 Check the **Device Name** check box from which you want to restore the configuration. Click **Restore**.

The **Devices** area shows the following fields:

- Device Name—Specifies the device name from which the configuration file is restored.
- IP Address—Specifies the IP Address of the device.
- Group—Specifies the group to which the device belongs.
- Status—Specifies the status of the device.

Note You can restore the configuration only from the same device. If you select user-imported configuration files, you can restore configuration for any number of devices.

Archive Jobs

This section contains context-sensitive online help content under Cisco DCNM **Configure > Backup > Switch Configuration >Archive Jobs**.



Note The configuration files from the archived jobs are located in the DCNM Server directory: `\dcm\dcnm\data\archive\<dcnm-ip-address>\`. You can use the third-party file transfer tools or file transfer commands to transfer these files to an external server.

The following table describes the fields that appear on the **Archive Jobs** window.

Field	Description
User	Specifies who created this job.
Group	Specifies the group to which this job belongs.
Group Job	Specifies whether it is a group job or a per-device job. The values are **true** or **false**.
Schedule	Specifies the schedule of the job. Also show the recurrence information.
Last Execution	Specifies the date and time at which this job was last executed.
Job Status	Specifies if the job was successful, scheduled, running, or failure. **Note** **Running** and **Scheduled** status is not applicable for existing jobs in an upgraded Cisco DCNM.
User Comments	Specifies the comments or description provided by the user.

Archive Jobs

To add, delete or view the job from the Cisco DCNM Web UI, perform the following steps:



Note You must set the SFTP/TFTP/SCP credentials before you configure jobs. On the DCNM Web Client, navigate to **Administration > DCNM Server > Archive FTP Credentials** to set the credentials.

Procedure

Step 1 Choose **Configure > Backup > Switch Configuration > Archive Jobs > Archive Jobs** tab, and click **Add Job**.

The Create Job screen displays the Schedule, Device Selection and Selected Devices.

A backup is scheduled as defined.

a) In the **Schedule** area, configure the start time, repeat interval and repeat days.

- **Start At**: Configure the start time using the hour:minutes:second drop-down lists.
  - **Once**: Configure the job to be executed once, on the particular day. The time at which this job will be executed is determined by the **Start At** field.
  - Now—Configure the job to be executed immediately. Cisco DCNM will consider the default date and time as configured on the server.

    Note You can schedule a job to run **Now** even if a job is already scheduled.

  - **Daily**: Check the check box on the days you want this job to be executed. The time at which this job will be executed is determined by the **Start At** field.
  - **Real Time**: Configure the job to be executed if there is any configuration changes in the device. The device must be quiet for 5 minutes, after which the DCNM Sever will execute this job.
- **Repeat Interval**: Check the Repeat Interval check box to repeat the job at scheduled intervals. Configure the intervals using either days or hours drop-down list.
- **Comments**: Enter your comments, if any.

b) In the **Device Selection** area, use the radio button to choose one of the following:

- **Device Group**: Click the Device Group radio button to select the entire group of devices for this job.

  Select the Device Group from the drop-down list.

  Note When the devices are not licensed, they will not be shown under the group on the Cisco DCNM **Configure > Backup > Switch Configuration > Archive Jobs**. When none of the devices under a group is licensed, the group alone will be shown with no devices, until a device under that group is licensed.

- **Selected Devices**: Click the **Selected Devices** radio button to select one of multiple devices from various groups for this job.

Select the devices from the drop-down list.

From Cisco DCNM Release 11.2(1), you can apply VRF for all the selected devices simultaneously. You can either apply Management VRFs or Default VRFs.

Note When the SAN and LAN credentials are not configured for a switch, it will not be listed in the Selected Devices drop-down list. To configure, navigate to **Administration > Credentials Management > SAN Credentials** and **Administration > Credentials Management > LAN Credentials**.

c) In the **Selected Devices** area, the following fields are shown:

- **Name**: Specifies the name of the device on which the job is scheduled.
- **IP Address**: Specifies the IP Address of the device.
- **Group**: Specifies the group to which the device belongs.
- **VRF**: Specifies the virtual routing and forwarding (VRF) instance.

  Select a VRF type to modify the existing VRF type to the specified device. You can either apply Management VRFs or Default VRFs.

Note If a job for a device exists under device level, you can create a group level job which includes this switch as part of that group. However, this switch will be excluded during the execution of the job.

d) Click **Create** to add a new job.

Step 2 To delete a job, from the Cisco DCNM home page, choose **Configure > Backup > Switch Configuration > Archive Jobs > Archive Jobs**, and select a job.

a) Click **Delete Job**.

The Schedule, Device Selection and the Selected devices for this job is displayed.

b) Click **Delete**.

Step 3 To view the details of the job, from the Cisco DCNM home page, choose **Configure > Backup > Switch Configuration > Archive Jobs > Archive Jobs**, and check the job check box.

a) Click **View/Modify Job**.

The Schedule, Device Selection and the Selected devices for this job is displayed.

b) Modify the required details. Click **OK** to revert to view the list of jobs.

Note
- You cannot modify a job that is scheduled to be run **Now** to one that is scheduled to be run **Daily**.
- You cannot modify the repeat interval duration for an archive job. When you try to modify, the operation fails and the job is deleted. You must delete existing repeat interval archive job and create a new job.

What to do next

You can also configure the Cisco DCNM to retain the number of archived files per device. Choose **Administration > DCNM Server > Server Properties**, and update the **archived.versions.limit** field.

Job Execution Details

The Cisco DCNM **Web Client > Configure > Backup > Switch Configuration > Archive Jobs > Archive Jobs > Job Execution Details** tab shows the following tabs in the Job Execution History table.

Field	Description
Job Name	Displays the system-generated job name.
User	Specifies the persona of the person who created the job.
Device 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.
Protocol	Specifies if the SFTP, TFTP, or SCP protocol is applied.
Execution time	Specifies the time at which the job was last executed.
Status	Specifies the status of the job. • Skipped • Failed • Successful
Error Cause	Specifies the error if the job has failed. The categories are as follows: • No change in the configuration. • Switch is not managed by this server. **Note** If the error cause column is empty, it implies that the job was executed successfully. Hover over the error cause to view the complete description.

Archives

A user with network operator role can view configuration archives for a switch and their details in the **Archives** window.

The following tables describe the icons and fields that are displayed in this window.

Table 20: Archive Operations

Icon	Description
Compare	Allows you to compare two configuration files either from different devices or on the same device.
View	Allows you to view a configuration file.

Table 21: Archive Field and Description

Field Name	Description
Device Name	Displays the device name Click on the arrow next to the device to view the configuration files.
IP Address	Displays the IP address of the device.
Group	Displays the group of the device.
Configuration	Displays the configuration files that are archived for that device.
Archive Time	Displays the time at which the device configuration files were archived. The format is Day:Mon:DD:YYYY HH:MM:SS.
Size	Displays the size of the archived file.

This section contains the following:

Compare Configuration Files

You can compare one version of a configuration file with another version of the same configuration file in the same device, or the configuration files of two different devices.

To compare the configuration files from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Backup > Archives**.

Step 2 In the **Archives** area, click the arrow that is adjacent the name of the device whose configuration files you want to view. The list of configuration files is displayed.

Step 3 Check the check box next to configuration files and select two configuration files to compare.

The first file that you select is designated as the source and the second configuration file is designated as the target file.

Step 4 Click **Compare**.

The **View Config Diff** page displays the difference between the two configuration files.

The Source and Target configuration files content are displayed in two columns. Choose **All** from the drop-down list in the right-top corner to view the entire configuration. Choose **Changed** to view the configuration differences between the configuration files.

The differences in the configuration files are shown in a table, with legends.

- **Red**: Deleted configuration details.
- **Green**: New added configuration.
- **Blue**: Modified configuration details.

View Configuration

You can view an archived configuration file.

To view or edit the configuration file for the devices from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Backup** > **Archives**.

The **Archives** window is displayed.

Step 2 Click the arrow that is next to the name of the device whose configuration files you want to view.

The list of configuration files are displayed.

Step 3 Select the radio button that is next to the corresponding file you want to view.

Step 4 Click the **View** configuration icon.

The **View** configuration window appears showing the configuration file content in the right column.

Network Config Audit

Cisco DCNM provides auditing for the configuration changes across the network switches. The Network Audit Reporting feature enables you to a generate audit report so that you can track the added, deleted, or modified configurations. You will be able to generate the network audit reports only when you have existing archival jobs. Using the generated reports, you can view the config differences on a device for a specified period.

This section contains the following:

Generating Network Config Audit Reports

To generate the network config audit reports from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Backup > Network Config Audit**.

The **Network Audit Report** window is displayed.

Step 2 In the **Devices** drop-down list, choose the devices to generate a report.

Step 3 Specify the **Start Date** and the **End Date**.

Step 4 Click **Generate Report** to view the configuration differences. The configuration differences are color-coded.

- Red: Deleted Configuration
- Green: Newly Added Configuration
- Blue: Changed configuration
- Strikethrough: Old configuration

After you generate a report, you can export the configuration reports into an HTML file.

Creating a Network Config Audit Report

To create a network config audit job and view the configuration differences between the devices from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor > Report > Generate**.

The left pane shows various reports that you can create.

Step 2 Choose **Common > Network Config Audit**.

Step 3 In the **Report Name** field, enter the name of the report.

Step 4 In the **Repeat** field, choose the appropriate repeat interval, that is, Daily, Weekly, or Monthly.

Daily job generates a report of configuration differences for all the selected devices for last 1 day. Weekly job generates a report for the last 7 days, and the monthly job generates a report for the last 30 days.

Step 5 In the **Start** and **End** date fields, specify the start and end date for the report.

Step 6 In the **Email Report** field, specify the email delivery options.

- No: Select this option if you do not want to send the report through email.
- Link Only: Select this option if you want to send the link to the report.
- Contents: Select this option if you want to send the report content.

If you select Link Only or the Contents option, enter the email address and subject in the **To** and **Subject** fields.

Monitoring Network Config Audit Report

To monitor the network config audit report from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **Report** > **View**.

Step 2 Choose **Common** > **Network Config Audit** in the left pane to the network config audit reports.

Deleting a Network Config Audit Report

To delete a network config audit report from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Monitor** > **Report** > **View**.

Step 2 Choose **Common** > **Network Config Audit**.

The **View Reports** window is displayed with the reports that you have created.

Step 3 Select the reports that you want to delete, and click the **Delete** icon.

Image Management

Upgrading your devices to the latest software version manually might take a long time and prone to error, which requires a separate maintenance window. To ensure rapid and reliable software upgrades, image management automates the steps associated with upgrade planning, scheduling, downloading, and monitoring. Image management is supported only for Cisco Nexus switches.

Note Before you upgrade, ensure that the POAP boot mode is disabled for Cisco Nexus 9000 Series switches and Cisco Nexus 3000 Series switches. To disable POAP, run the `no boot poap enable` command on the switch console. You can however, enable it after the upgrade.

The **Image Management** menu includes the following submenu:

Upgrade [ISSU]

The **Upgrade [ISSU]** menu includes the following submenus:

Upgrade History [ISSU]

This feature enables you to upgrade the Cisco Nexus Platform Switches using In-Service Software Upgrade (ISSU). This upgrade procedure may be disruptive or non-disruptive based on the device configuration. You can select the Kickstart, System, or SSI images required for the upgrade from a remote server using SFTP, SCP, TFTP, FTP or from image repository or the file system on the device. Image repository can use SCP, SFTP, FTP, or TFTP as file transfer protocol. To select the images from the repository, the same needs to be uploaded from **Configure** > **Image Management** > **Repositories** tab.

The following table describes the fields that appear on **Configure > Image Management > Upgrade [ISSU] > Upgrade History**.

Field	Description
Task Id	Specifies the serial number of the task. The latest task will be listed in the top. **Note** If Failover is triggered in Native HA, the Task Id sequence number is incremented by 32.
Task Type	Specifies the type of task. • Compatibility • Upgrade
Owner	Based on the Role-Based Authentication Control (RBAC), specifies the owner who initiated this task.
Devices	Displays all the devices that were selected for this task.
Job Status	Specifies the status of the job. • Planned • In Progress • Completed • Completed with Exceptions **Note** If the job fails on a single or multiple devices, the status field shows COMPLETED WITH EXCEPTION indicating a failure.
Created Time	Specifies the time when the task was created.
Scheduled At	Specifies the time when the task is specified to be executed. You can also choose to schedule a task to be executed at a later time.
Completed Time	Specifies the time when the task was completed.
Comment	Shows any comments that the Owner has added while performing the task.



Note After a fresh Cisco DCNM installation, this page will have no entries.

You can perform the following:

New Installation

To upgrade the devices that are discovered from the Cisco DCNM, perform the following steps:

Procedure

Step 1 Choose **Configure > Image Management > Upgrade [ISSU] > Upgrade History**.

Step 2 Choose **New Installation** to install, or upgrade the kickstart and the system images on the devices.

The devices with default VDCs are displayed in the **Select Switches** window.

Step 3 Select the check box to the left of the switch name.

You can select more than one switch and move the switches to the right column.

Step 4 Click **Add** or **Remove** icons to include the appropriate switches for upgrade.

The selected switches appear in a column on the right.

Step 5 Click **Next**.

The **Specify Software Images** window appears. This tab displays the switches that you selected in the previous screen. You can choose the images for upgrade as well.

- The **Auto File Selection** check box enables you to specify a file server, an image version, and a path where you can apply the upgraded image to the selected devices.
- In the **Select File Server** drop-down list, select the one of the file servers that is created in the Cisco DCNM repositories.
- In the **Image Version** field, specify the image version. For example, enter 7.3.9.D1.1 in the **Image Version** field if you have selected m9700-sf3ek9-kickstart-mz.7.3.0.D1.1.bin as the image version.
- In the **Path** field, specify the image path. Specify an absolute path if you choose SCP or SFTP. For example, `//root/images/`. Specify a relative path to the FTP or TFTP home directory if you choose FTP or TFTP. Specify the absolute path of the image if you're using TFTP server that is provided by Cisco DCNM, local DCNM TFTP. You can't use the same DCNM TFTP server for creating another job when the current job is in progress.

Step 6 Click **Select Image** in the **Kickstart image** column.

The **Software Image Browser** dialog box appears.

Note
- Cisco Nexus 3000 Series and 9000 Series Switches require only the system image to load the Cisco NX-OS operating system. Therefore, the option to select kickstart images for these devices is disabled.
- If there's an issue in viewing the **Software Image Browser** dialog box, reduce the font size of your browser and retry.

Step 7 Click **Select Image** in the **System Image** column.

The **Software Image Browser** dialog box appears.

Step 8 On the **Software Image Browser** dialog box, you can choose the image from **File Server** or **Switch File System**.

If you choose **File Server**:

a) From the **Select the File server** list, choose the appropriate file server on which the image is stored.

The servers at **Configure > Image Management > Repositories** are displayed in the drop-down list.

b) From the **Select Image** list, choose the appropriate image. Check the check box to use the same image for all other selected devices of the same platform.

Example: For platform types N7K-C7009 and N7K-C7010, logic matches platform (N7K) and three characters (C70) from subplatform. The same logic is used across all platform switches.

Note Only files with BIN extension are listed if you select **File Server**. To view other files, choose **Administration > DCNM Server > Server Properties**, set **FILE_SELECTION_FILTER** to **false**, and restart the server. It is set to **true** by default.

c) Click **OK**.

If the file server selected is either `ftp` or `tftp`, in the text box, enter the relative path of the file from the home directory.

If you choose **Switch File System**:

a) From the **Select Image** list, choose the appropriate image that is located on the flash memory of the device.

Note Only files with BIN extension are listed if you select **Switch File System**. To view other files, choose **Administration > DCNM Server > Server Properties**, set **FILE_SELECTION_FILTER** to **false**, and restart the server. It is set to **true** by default.

b) Click **OK** to choose the kickstart image or **Cancel** to revert to the **Specify Software Images** dialog box.

Step 9 The **Vrf** column indicates the name of the virtual routing and forwarding (VRF).

Step 10 In the **Available Space** column, specify the available space for the **Primary Supervisor** and **Secondary Supervisor** modules of the switch.

Available Space column shows the available memory in MB on the switch (for less than 1 MB, it's shown and marked as KB).

Bootflash browser shows the filename, size, and last modified date for all the files and directories on the switch bootflash. You can delete files by selecting them and clicking **Delete** to increase the available space on the switch.

Step 11 **Selected Files Size** column shows the size of images that are selected from the SCP or SFTP server.

If the total size of selected images is greater than available space on a switch, the file size is marked in red. We recommend that you create more space on the switch to copy images to it and install.

Step 12 Drag and drop the switches to reorder the upgrade task sequence.

Step 13 Select **Skip Version Compatibility** if you are sure that the version of the Cisco NX-OS software on your device is compatible with the upgraded images that you have selected.

Step 14 Select **Select Parallel Line Card upgrade** to upgrade all the line cards at the same time.

Upgrading a parallel line card isn't applicable for Cisco MDS devices.

Step 15 Click **Options** under the **Upgrade Options** column to choose the type of upgrade.

Upgrade Options window appears with two upgrade options. The drop-down list for **Upgrade Option 1** has the following options:

- **NA**
- **bios-force**
- **non-disruptive**

NA is the default value.

The drop-down list for **Upgrade Option 2** has the following options:

- **NA**
- **bios-force**

When **NA** is selected under **Upgrade Option 1**, **Upgrade Option 2** is disabled.

When you choose **bios-force** under **Upgrade Option 1**, **Upgrade Option 2** is disabled.

When **non-disruptive** is selected under **Upgrade Option 1**, you can choose **NA** or **bios-force** under **Upgrade Option 2**.

Check the **Use this Option for all other selected devices** check box to use the selected option for all the selected devices and click **OK**.

Note
- The upgrade options are applicable only for Cisco Nexus 3000 Series and 9000 Series switches.
- Selecting the **non-disruptive** option for upgrading does not ensure a non-disruptive upgrade. Perform a compatibility check to ensure that the device supports non-disruptive upgrade.

Step 16 Click **Next**.

If you didn't select **Skip Version Compatibility**, the Cisco DCNM performs a compatibility check.

You can choose to wait until the check is complete or click **Finish Installation Later**.

The installation wizard is closed and a compatibility task is created in **Configure > Image Management > Upgrade [ISSU] > Upgrade History** tasks.

The time that is taken to check the image compatibility depends on the configuration and the load on the device.

The **Version Compatibility Verification** status column displays the status of verification.

If you skip the version compatibility check by choosing **Skip Version Compatibility**, Cisco DCNM displays only the name of the device. The **Current Action** column displays **Completed**, and the **Version Compatibility Verification** column displays **Skipped**.

Step 17 Click **Finish Installation Later** to perform the upgrade later.

Step 18 Click **Next**.

Step 19 Check the **Next** check box to put a device in maintenance mode before upgrade.

Step 20 Check the check box to save the running configuration to the startup configuration before upgrading the device.

Step 21 You can schedule the upgrade process to occur immediately or later.

a. Select **Deploy Now** to upgrade the device immediately.

b. Select **Choose time to Deploy** and specify the time in MMM/DD/YYYY HH:MM:SS format to perform the upgrade later.

This value is relative to the server time. If the selected time to deploy is in the past, the job is executed immediately.

Step 22 You can choose the execution mode based on the devices and the line cards you have chosen to upgrade.

a. Select **Sequential** to upgrade the devices in the order you chose them.

b. Select **Concurrent** to upgrade all the devices at the same time.

Step 23 Click **Finish** to begin the upgrade process.

The Installation wizard closes and a task to upgrade is created on the **Configure > Image Management > Upgrade [ISSU] > Upgrade History** page.

What to do next

After you complete the ISSU on the switch, ensure that you wait for 20 minutes to allow the switch to reboot, and stabilize the SNMP agent. DCNM discovers polling cycles in order to display the new version of the switch on the Cisco DCNM Web UI.

Finish Installation

You can choose to complete the installation for tasks which was completed on the **Compatibility Check** page. Perform the following task to complete the upgrade process on the devices.

Procedure

Step 1 Choose **Configure > Image Management > Upgrade [ISSU] > Upgrade History**, select a task for which the compatibility check is complete.

Select only one task at a time.

Step 2 Click **Finish Installation**.

Software Installation Wizard appears.

Step 3 Check the check box to save the running configuration to the startup configuration before upgrading the device.

Step 4 Check the check box to put a device in maintenance mode before upgrade. This option is valid only for the devices that support maintenance mode.

Step 5 You can schedule the upgrade process to occur immediately or later.

a. Select **Deploy Now** to upgrade the device immediately.

b. Select **Choose time to Deploy** and specify the time in DD/MM/YYYY HH:MM:SS format to perform the upgrade later.

Step 6 You can choose the execution mode that is based on the devices and the line cards that you have chosen to upgrade.

a. Select **Sequential** to upgrade the devices in the order in which they were chosen.

b. Select **Concurrent** to upgrade the devices at the same time.

Step 7 Click **Finish** to complete the upgrade process.

View

To view the image upgrade history from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Image Management > Upgrade [ISSU] > Upgrade History**, check the task ID check box.

Select only one task at a time.

Step 2 Click **View**.

The **Installation Task Details** window appears.

Step 3 Click **Settings**. Expand the **Columns** menu and choose the details you want to view.

You can view the following information in this window:

- Location of the kickstart and system images
- Compatibility check status
- Installation status
- Descriptions
- Logs

Step 4 Select the device.

The detailed status of the task appears. For the completed tasks, the response from the device appears.

If the upgrade task is in progress, a live log of the installation process appears.

Note
- This table autorefreshes every 30 secs for jobs in progress, when you're on this window.
- The switch-level status for an ongoing upgrade on a Cisco MDS switch doesn't appear for other users without SAN credentials. To apply SAN Credentials, choose **Administration > Credentials Management > SAN Credentials**.

Delete

To delete a task from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Image Management > Upgrade [ISSU] > Upgrade History**, and check the **Task ID** check box.

Step 2 Click **Delete**.

Step 3 Click **OK** to confirm deletion of the job.

Switch Level History

You can view the history of the upgrade process at a switch level. You can view the current version of the switch and other details.

The following table describes the fields that appear on **Configure > Image Management > Upgrade [ISSU] > Switch Level History**.

Field	Description
Switch Name	Specifies the name of the switch
IP Address	Specifies the IP Address of the switch
Platform	Specifies the Cisco Nexus switch platform
Current Version	Specifies the current version on the switch software

Click the radio button next to a switch name to select the switch and view its upgrade history. Click **View** to view the upgrade task history for the selected switch.

The following table describes the fields that appear on **Configure > Image Management > Upgrade [ISSU] > Switch Level History > View Device Upgrade Tasks**:

Field	Description
Owner	Specifies the owner who initiated the upgrade.
Job Status	Specifies the status of the job. • Planned • In Progress • Completed
KickStart Image	Specifies the kickStart image that is used to upgrade the Switch.
System Image	Specifies the system image that is used to upgrade the switch.
Completed Time	Specifies the date and time at which the upgrade was successfully completed.
Status Description	Specifies the installation log information of the job.

Patch [SMU]

The Patch [SMU] menu includes the following submenus:

Installation History

This feature allows you to activate or deactivate packages using Software Maintenance Update (SMU). Personnel with Admin privileges can perform this operation.

The following table describes the fields that appear on **Configure > Image Management > Patch [SMU] > Installation History**.

Field	Description
Task Id	Specifies the serial number of the task. The latest task is listed at the top. The tasks are performed in the sequential order.
Switch Name	Specifies the name of the switch for which the patch file is installed.
IP Address	Specifies the IP Address of the device.
Task	Specifies if the patch is installed or uninstalled on this device.
Package	Specifies the name of the patch file.
Status	Specifies the status of installation or uninstallation of the patch files.
Status Description	Describes the status of installation or uninstallation of the patch files.

This section contains the following:

Install Patch

To install the patch on your devices from Cisco DCNM Web Client, perform the following steps:

Procedure

Step 1 Choose **Configure > Image Management > Patch [SMU] > Installation History**, click **Install**.

The **Select Switches** window appears. All the Cisco Nexus switches that are discovered by Cisco DCNM are displayed.

Step 2 Select the check box to the left of a switch name.

You can select more than one device.

Step 3 Click **Add** or **Remove** icons to include the appropriate switches for installing the patch.

The selected switches appear in the right column.

Step 4 Click **Next**.

Step 5 Click **Select Packages** in the **Packages** column.

The **SMU Package Browser** dialog box appears.

Step 6 In the **SMU Package Browser** dialog box, you can choose the patch file from **File Server** or **Switch File System**.

If you choose **File Server**:

a) From the **Select the file server** list, choose the appropriate file server on which the patch is stored.

The servers, which are listed in the **Repositories** window, are displayed in the drop-down list. Choose **Configure > Image Management > Repositories** to view the **Repositories** window.

b) From the **Select Image** list, choose the appropriate patch that must be installed on the device.

You can select more than one patch file to be installed on the device.

Note If the patch installation results in the restart of the device, select only one patch file.

Check the check box to use the same patch for all other selected devices of the same platform.

Only files with BIN extension are listed if you select **File Server**. To view other files, choose **Administration > DCNM Server > Server Properties**, set **FILE_SELECTION_FILTER** to **false**, and restart the server. It is set to **true** by default.

c) From the **Select Vrf** list, choose the appropriate virtual routing and forwarding (VRF).

The two options in the drop-down list are **management** and **default**.

Check the check box to use the same VRF for all other selected devices.

d) Click **OK** to choose the patch image or **Cancel** to revert to the SMU installation wizard.

If you choose **Switch File System**:

a) From the **Select Image** list, choose the appropriate patch file image that is located on the flash memory of the device.

You can select more than one patch file to be installed on the device.

Only files with BIN extension are listed if you select **Switch File System**. To view other files, choose **Administration > DCNM Server > Server Properties**, set **FILE_SELECTION_FILTER** to **false**, and restart the server. It is set to **true** by default.

b) Click **OK** to choose the image, **Clear Selections** to uncheck all the check boxes, or **Cancel** to revert to the **SMU Package Browser** dialog box.

Step 7 Click **Finish**.

You will get a confirmation window. Click **OK**.

Note SMU installation may reload the switch if the SMU is reloaded.

You can view the list of patches that are installed on the switch in the **Switches** window by choosing **DCNM > Inventory > Switches**.

Uninstall Patch

To uninstall the patch on your devices from Cisco DCNM Web Client, perform the following steps:

Procedure

Step 1 Choose **Configure > Image Management > Patch [SMU] > Installation History**, click **Uninstall**.

The **Select Switches** page appears. The discovered Cisco Nexus switches are displayed.

Step 2 Check the check box on the left of the switch name.

You can select more than one image device.

Step 3 Click **Add** or **Remove** icons to include the appropriate switches for installing the patch.

The selected switches appear in a column on the right.

Step 4 Click **Next**.

The **Active Packages** page appears.

Step 5 Click **Select Packages** under the **Installed Packages** column.

The **Packages Installed** window appears, which lists the patches that are applied to the switch.

Step 6 Select the patches that you want to uninstall from this device.

You can select more than one patch that is applied on the device.

Note If the patch uninstallation results in the restart of the device, select only one patch.

Step 7 Click **Finish** to uninstall the patch from the device.

You will get a confirmation window. Click **OK**.

You can uninstall more than one patch at a time.

Note SMU uninstallation may reload the switch if the SMU is reloaded.

Delete Patch Installation Tasks

To delete the patch installation tasks from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Image Management > Patch [SMU] > Installation History**, check the task ID check box.

Step 2 Click **Delete**.

Step 3 Click **OK** to confirm deletion of the patch installation task.

Switch Installed Patches

You can view the patches that are installed on all the switches in the network. You can refresh the view to see the latest installed patches.

The following table describes the fields that appear on **Configure > Image Management > Patch [SMU] > Switch Installed Patches**.

Field	Description
Switch Name	Specifies the name of the switch.
IP Address	Specifies the IP address of the switch.
Platform	Specifies the Cisco Nexus switch platform.
Installed Patches	Specifies the currently installed patches on switches.

Click **Refresh** to refresh the table.

Package [RPM]

The Package [RPM] menu includes the following submenus:

Package Installation [RPM]

The package [RPM] feature allows you to install RPM packages. This feature is available for the Cisco Nexus 9000 Series and 3000 Series Switches.

The following table describes the fields that appear on **Configure > Image Management > Package [RPM] > Installation History**.

Field	Description
Task Id	Specifies the serial number of the task. The latest task is listed in the top. The tasks are performed in the sequential order.
Switch Name	Specifies the name of the switch for which the package file is installed.
IPAddress	Specifies the IP address of the device.
Task	Specifies if the package is installed or uninstalled on this device.
Package	Specifies the name of the package file.
Status	Specifies the status of installation or uninstallation of the package files.
Completed Time	Specifies the time at which the installation or uninstallation task completed.
Status Description	Describes the status of installation or uninstallation of the package files.

This section contains the following:

Install Package [RPM]

Perform the following task to install the package on your devices using Cisco DCNM Web client.

Procedure

Step 1 Choose **Configure > Image Management > Package [RPM] > Installation History**, click **Install**.

The **Select Switches** page appears.

Step 2 Check the check box on the left of the switch name.

You can select more than one device.

Step 3 Click **Add** or **Remove** to include appropriate switches for installing packaging.

The selected switches appear in a column on the right.

Step 4 Click **Next**.

Step 5 Click **Select Packages** in the **Packages** column.

The **RPM Package Browser** screen appears.

Step 6 Choose the package file from **File Server** or **Switch File System**.

If you choose **File Server**:

a) From the **Select the file server** list, choose the appropriate file server on which the package is stored.

The servers at **Configure > Image Management > Repositories** are displayed in the drop-down list.

b) From the **Select Image** list, choose the appropriate package that must be installed on the device.

You can select more than one package file to be installed on the device.

Only files with RPM extension are listed if you select **File Server**. To view other files, choose **Administration > DCNM Server > Server Properties**, set **FILE_SELECTION_FILTER** to **false**, and restart the server. It is set to **true** by default.

Check the check box to use the same package for all other selected devices of the same platform.

c) Click **OK** to choose the patch image or **Cancel** to revert to the RPM Installation Wizard.

If you choose **Switch File System**:

a) From the **Select Image** list, choose the appropriate package file image that is located on the flash memory of the device.

You can select more than one package file to be installed on the device.

Only files with RPM extension are listed if you select **Switch File System**. To view other files, choose **Administration > DCNM Server > Server Properties**, set **FILE_SELECTION_FILTER** to **false**, and restart the server. It is set to **true** by default.

b) Click **OK**.

Step 7 In the **Installation Type** column, choose one of the installation types:

- **Normal**—Fresh installation
- **Upgrade**—Upgrading the existing RPM

- **Downgrade**—Downgrading the existing RPM

Step 8 Click **Finish**.

You can view the list of packages that are installed on the switch, on the **Web Client > Inventory > Switches** page.

Note If you are using Cisco DCNM Release 10.1(2), in case of installation of reload RPMs, perform a manual install commit on the switch after it switch reloads.

Uninstall Package [RPM]

To uninstall the RPM on your devices from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Image Management > Package [RPM] > Installation History**, click **Uninstall**.

The **Select Switches** window appears.

Step 2 Check the check box on the left of the switch name.

You can select more than one switch.

Step 3 Click the **Add** or **Remove** icons to include the appropriate switches for uninstalling the package.

The selected switches appear in a column on the right.

Step 4 Click **Next**.

The **Active Packages** page appears.

Step 5 Click **Select Packages** under the **Installed Packages** column.

The **Packages Installed** window appears, which lists the packages that are installed in the switch.

Step 6 Click **Finish** to uninstall the package from the device.

You will get a confirmation window. Click **OK**.

You can uninstall more than one package at a time.

Note
- If you are using Cisco DCNM Release 10.1(2), in case of uninstallation of reload RPMs, a manual install commit needs to be performed on the switch once the switch is reloaded.
- RPM uninstallation may reload the switch if the RPM is reload RPM.

Delete Package Installation Tasks

To delete the package installation tasks from the history view from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Image Management > Package [RPM] > Installation History**, select the task ID check box.

Step 2 Click **Delete**.

Step 3 Click **OK** to confirm deletion of the task.

Switch Installed Packages

You can view the RPM packages that are installed on all Switches in the network. You can refresh the view to see the latest installed packages.

The following table describes the fields that appear on **Configure > Image Management > Packages [RPM] > Switch Installed Packages**.

Field	Description
Switch Name	Specifies the name of the switch.
IP Address	Specifies the IP address of the switch.
Platform	Specifies the Cisco Nexus switch platform.
Installed Packages	Specifies the currently installed packages on the switches and the type of package. The installed packages can be base packages or non-base packages.

Click **Refresh** to refresh the table.

Maintenance Mode [GIR]

The Maintenance Mode [GIR] menu includes the following submenus:

Maintenance Mode

The maintenance mode allows you to isolate the Cisco Nexus Switch from the network to perform an upgrade or debug, using Graceful Insertion and Removal (GIR). When the switch maintenance is complete, you can return the switch to normal mode. When the switch is in the maintenance mode, all protocols are gracefully brought down and all physical ports are shut down. When the normal mode is restored, all the protocols and ports are initiated again.

Perform the following to change the system mode of the devices.

Procedure

Step 1 Choose **Configure > Image Management > Maintenance Mode [GIR] > Maintenance Mode**, check the switch name check box.

You can select multiple switches.

Step 2 Choose one of the following options under the **Mode Selection** column:

- Shutdown
- Isolate

Note Click the appropriate option before you change the mode.

Step 3 Click **Change System Mode**.

A confirmation message appears.

Step 4 Click **OK** to confirm to change the maintenance mode of the device.

The status of operation can be viewed in the **System Mode** and the **Maintenance Status**.

Switch Maintenance History

You can view the history of the maintenance mode changes executed from the Cisco DCNM.

The following table describes the fields that appear on **Configure > Image Management > Maintenance Mode [GIR] > Switch Maintenance History**.

Field	Description
Task Id	Specifies the serial number of the task. The latest tasks that are listed in the top.
Switch Name	Specifies the name of the switch for which the maintenance mode was changed.
IP Address	Specifies the IP address of the switch.
User	Specifies the name of the user who initiated the maintenance.
System Mode	Specifies the mode of the system.
Maintenance Status	Specifies the mode of the maintenance process.
Status	Specifies the status of the mode change.
Completed Time	Specified the time at which the maintenance mode activity was completed.

Click the radio button next to the switch name to select the switch for which you need to view the upgrade history. Click **View** to view the upgrade task history for the selected switch.

The following table describes the fields that appear on **Configure > Image Management > Upgrade [ISSU] > Switch Level History > View > Upgrade Tasks History**

Field	Description
Owner	Specifies the owner who initiated the upgrade.

Field	Description
Job Status	Specifies the status of the job. • Planned • In Progress • Completed
KickStart Image	Specifies the kickstart image that is used to upgrade the Switch.
System Image	Specifies the system image that is used to upgrade the switch.
Completed Time	Specifies the date and time at which the upgrade was successfully completed.

Image and Configuration Servers

This feature allows you to upload or delete images that are used during POAP and switch upgrade. To view the **Image and Configuration Servers** window from the Cisco DCNM Web UI homepage, choose **Configure > Image Management > Repositories**.

You can view the following details in the **Image and Configuration Servers** window.

Field	Descriptions
Name	Specifies the name of the repository you upload.
URL	Specifies the path where you uploaded the repository.
Username	Specifies the username of the remote server.
Last Modified	Specifies the date and timestamp of the last modification.

Add Image or Configuration Server URL

To add an image or a configuration server URL to the repository from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 On the **Image and Configuration Servers** window, click the **Add** icon.

The **Add Image or Configuration Server URL** window is displayed.

Step 2 Specify a name for the image.

Step 3 Click the radio button to select the protocol.

The available protocols are **SCP**, **FTP**, **SFTP**, and **TFTP**. Use the SCP protocol for POAP and Image Management.

You can use IPv4 and IPv6 addresses with these protocols.

Step 4 Enter the hostname or IP address and the path to download or upload files.

Note If you choose **SCP** or **SFTP** protocol and the path is root or /directory, adding an image or configuration server will not be successful.

Step 5 Specify the username and password.

Step 6 Click **OK** to save.

Deleting an Image

To delete an image from the repository from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure** > **Image Management** > **Repositories**.

The **Image and Configuration Servers** window appears.

Step 2 Choose an existing image from the list and click the **Delete Image** icon.

A confirmation window appears.

Step 3 Click **Yes** to delete the image.

Editing an Image or Configuration Server URL

To edit an image or a configuration server URL to the repository from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 On the **Image and Configuration Servers** window, select an existing image and configuration server from the list, and click **Edit**.

Step 2 In the **Edit Image or Configuration Server URL** window, edit the required fields.

Step 3 Click **OK** to save or click **Cancel** to discard the changes.

File Browser

You can view the contents of the server on the **Image and Configuration Servers** page.

1. In the **Image and Configurations** page, check the **Server Name** check box to view the content.

2. Click **File Browser** to view the contents of this server.

Image Upload

To upload different types of images to the server from the Cisco DCNM Web UI, perform the following steps:



Note Devices use these images during POAP or image upgrade.

Your user role should be **network-admin** to upload an image. You can't perform this operation with the **network-stager** user role.

Procedure

Step 1 Choose **Configure** > **Image Management** > **Repositories**.

The **Image and Configuration Servers** window appears.

Step 2 Click **Image Upload**.

The **Select File to Upload** dialog box appears.

Step 3 Click **Choose file** to choose a file from the local repository of your device.

Step 4 Choose the file and click **Upload**.

Step 5 Click **OK**.

The upload takes some time depending on the file size and network bandwidth.

LAN Telemetry Health

Starting from DCNM 11.2(1), Streaming LAN Telemetry preview feature in DCNM is obsolete and is replaced by Network Insights Resources (NIR) application. NIR can be deployed using Cisco DCNM Applications Framework on **Web UI** > **Applications**. After the NIR is enabled on a fabric, you can monitor the status on the window in the Cisco DCNM Web UI.

When the connection status is shown as **Disconnected** the port configuration may not be accepted by the switch correctly. On the switch image 7.0(3)I7(6), if a switch already had **nxapi** configuration, and later it was managed by DCNM and telemetry was enabled on that fabric, DCNM pushes **http port 80** configuration so that it could query some NXAPI commands such as **show telemetry transport** and **show telemetry data collector details**, to monitor telemetry connection statistics. In this case, the switch does not update **http port 80** in its configuration even though the command was executed correctly. In such a scenario, issue the following commands on the switch:

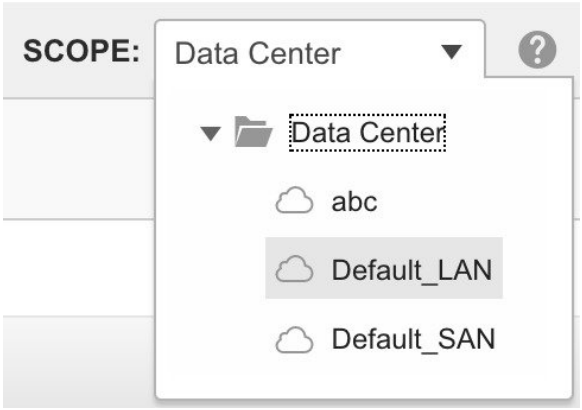
```
switch# configure
switch(config)# no feature nxapi
switch(config)# feature nxapi
switch(config)# http port 80
```

Note ICAM telemetry commands such as forwarding TCAM and ACL TCAM are not supported on Cisco Nexus C9504, C9508, and C9516 Series platforms for switch images 7.0(3)I7(5) and 7.0(3)I7(6)

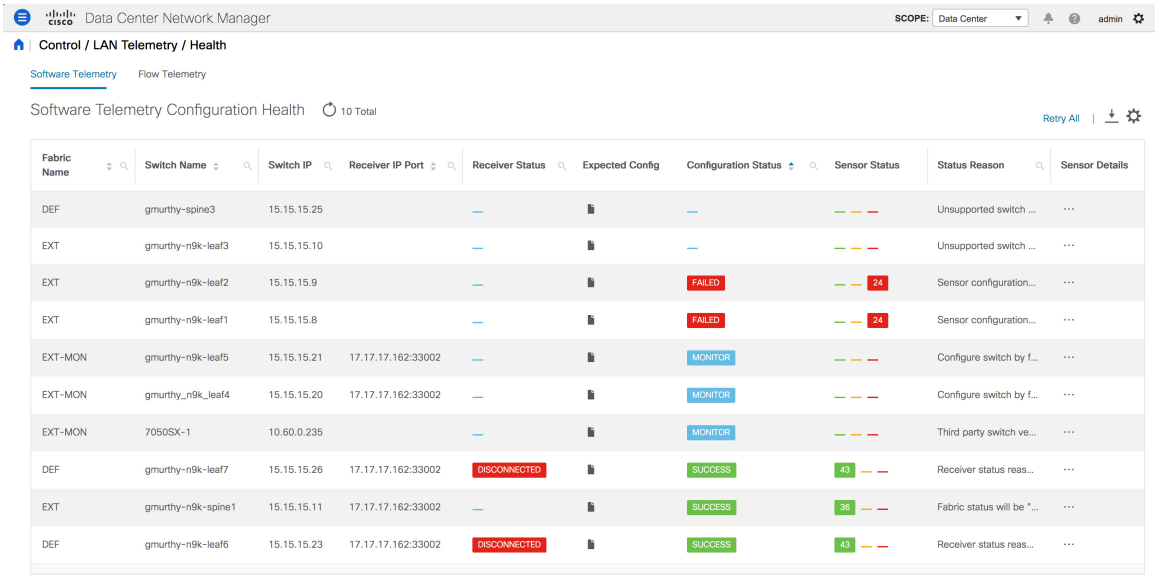
LAN Telemetry has the following topics:

Health

Cisco DCNM allows you to monitor the configuration health attributes of Software Telemetry and Flow Telemetry for each fabric. The attributes are displayed for a particular fabric or all fabrics based on the selected **SCOPE**. **Data Center scope** displays all fabrics by default.



Software Telemetry



The following table describes the fields that appear in the **LAN Telemetry > Health > Software Telemetry** window.

Field	Description
Fabric Name	Displays the fabric name.
Switch Name	Displays the switch name.
Switch IP	Displays the switch management IP address.
Switch Serial	Displays the switch serial number. This column is hidden by default. Click the **Settings** icon, and check the **Switch Serial** check box to add it to the columns displayed.
Switch Model	Displays the switch model. This column is hidden by default. Click the **Settings** icon, and check the **Switch Model** check box to add it to the columns displayed.
Switch Version	Displays the switch image version. This column is hidden by default. Click the **Settings** icon, and check the **Switch Version** check box to add it to the columns displayed.
Receiver IP Port	Displays the receiver IP and port assigned to a switch to transport telemetry data. The assigned IP and port will be based on the configured telemetry network, out-of-band or in-band, and the corresponding receiver microservice that is running in NIR application.

Field	Description

Receiver Status	Displays the status of the connection used to transport telemetry data between the switch and the receiver running in the NIR application.
	
	The telemetry manager polls the switch for the connection status every 5 mins.
	
	The valid values are:
	
	• **Connected**: The status is **Connected** when the telemetry manager is able to poll the receiver connection status from the switches.
	
	• **Disconnected**: If the status is **Disconnected**, the reason is mentioned in the **Status Reason** column.
	
	• **Null**: The status is **Null** when the telemetry manager in DCNM has not polled the receiver connection status from the switches or when it has not received any response from the switch for that request. When the receiver status is **Null** and if the configuration status is **MONITOR** or **SUCCESS**, log into the switch and check the nxapi configuration.
	
	When you enable telemetry on a fabric that is managed by DCNM, the telemetry manager pushes the **httpport 80** configuration. If the switch does not have **httpport 80** configuration, run the following commands on the switch:
	
	`switch# configure terminal`
	`switch(config)# no feature nxapi`
	`switch(config)# feature nxapi`
	`switch(config)# http port80`

Configuration Type	Displays the connection type ex: gRPC as reported by the switch. This value is obtained as part of the receiver connection status response from the switch. This column is hidden by default. It can be selected by clicking on the settings button.

Field	Description
Expected Config	Click the **Expected Config** icon to view the expected configuration for the switch in a dialog box. In case of error, the error reason will be displayed in the output.

Expected Switch Configuration (Fabric: EXT, Switch: gmurthy-n9k-spine1)

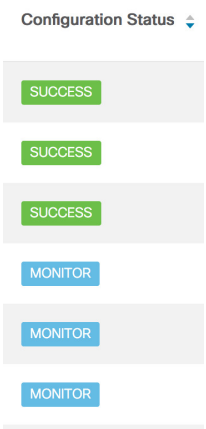
```
configure terminal

feature nxapi
nxapi http port 80

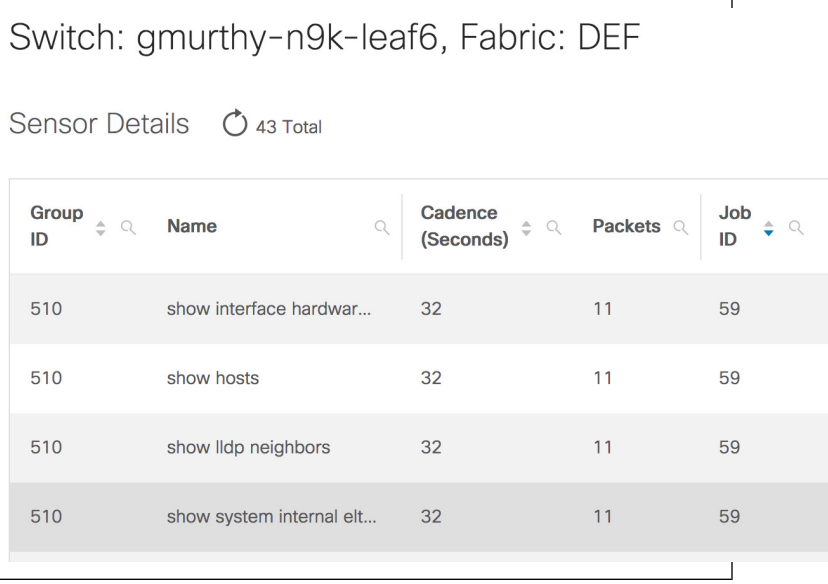
feature ntp
ntp server 15.15.15.162 prefer use-vrf management

feature lldp
feature icam
feature telemetry

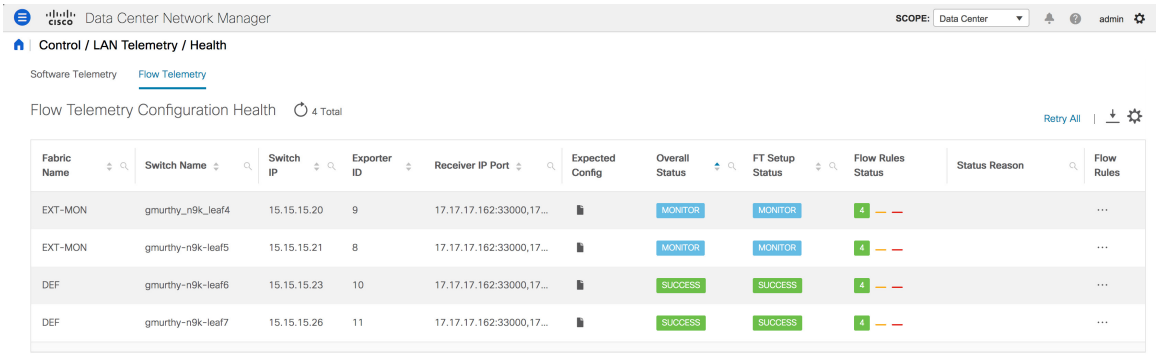
telemetry
  destination-profile
    use-vrf default
    source-interface loopback0
  destination-group 500
    ip address 17.17.17.162 port 33002 protocol gRPC encoding GPB
  sensor-group 508
    data-source DME
    path sys/intf depth 1 query-condition query-target=subtree&target-subtree-class=
query-target-filter=deleted()
```

Field	Description
Configuration Status	Displays the telemetry configuration switch summary status. The valid values are: • **MONITOR**: Implies that the switch in the fabric was configured as **Monitored** in the NIR app. In this case, configure these switches manually with the telemetry configurations as displayed in the **Expected Config** column. • **PROCESSING**: Implies that the switch belonging to the fabric was configured as **Managed** in the NIR app. In this case, the telemetry manager will configure the switches and when configuration is in progress, it is displayed as **PROCESSING**. • **SUCCESS**: Implies that the switches were successfully configured. • **PARTIAL SUCCESS**: Implies that some of the telemetry configurations could not be pushed to the switches. The **Status Reason** column will indicate the failure reason. • **FAILED**: Implies that the DCNM job failed to configure the switches. It could happen that some configuration did get pushed to the switches while some did not, in that case also DCNM marks the whole job as **Failed**. The **Status Reason** column will indicate the failure reason. You can filter the switches based on a particular status using the search option or you can sort the switches based on the status. 

Field	Description
Sensor Status	Displays the sensor configuration status in a distributed color format. The sensor count is divided into three categories: • Green color (Success): Number of sensor paths that got configured successfully • Yellow color (Pending): Number of sensor paths that are pending to be configured • Red color (Failed): Number of sensor paths that could not be configured
Status Reason	Displays the failure reasons for telemetry configuration status and receiver connection status or other information.

Field	Description
Sensor Details	Displays the following sensor details: • **Group ID**: The group ID to which the sensor path belongs • **Name**: The sensor path name as seen on the switch, for example: **show processes cpu** • **Cadence (Seconds)**: The sample interval, in seconds, at which the switch streams that sensor path. For example: If the value is 60, every 60 seconds the switch shall stream that sensor metric. • **Packets**: Specifies the number of metric samples that is collected till time. • **Job ID**: This is the DCNM telemetry job ID that was used to configure the sensor path on the switch. • **Status**: The status of the job. • **Status Reason**: The status reason of the job. In case the job failed, it specifies the failure reason of that job. 

Flow Telemetry



The following icons appear in the **LAN Telemetry > Health > Flow Telemetry** window.

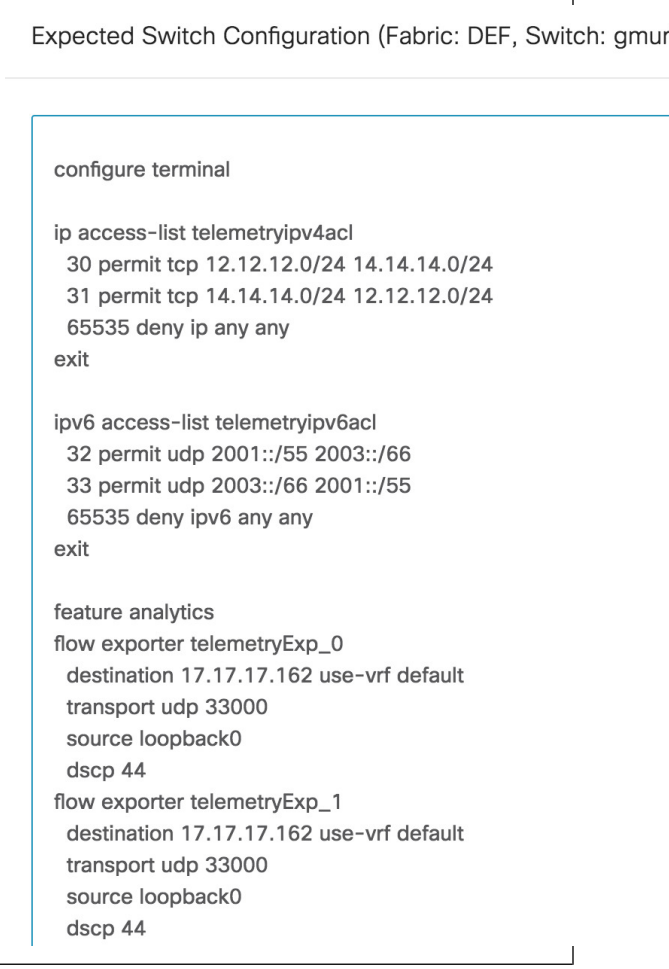
- **Retry All**: Click the **Retry All** icon to retry the failed configurations on the switches. However, this option does not fix the issue for the unsupported configurations automatically.
- **Export**: Click the **Export** icon to download the data in a spreadsheet.
- **Settings**: Click the **Settings** icon to add or delete the columns you want to view.

The following table describes the columns in the **LAN Telemetry > Health > Flow Telemetry** tab.

Table 22: Fields and Description on Flow Telemetry Health tab

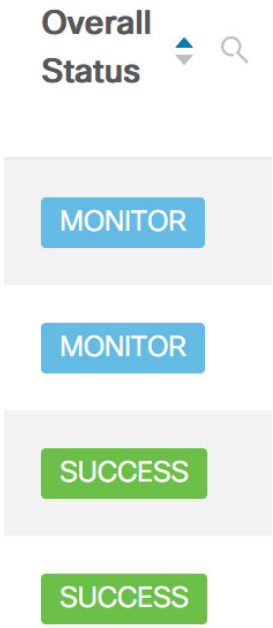
Field	Description
Fabric Name	Displays the name of the fabric.
Switch Name	Displays the name of the switch.
Switch IP	Displays the switch management IP address.
Switch Serial	Displays the serial number of the switch. By default, this column is hidden. It can be selected by clicking the Settings button.
Switch Model	Displays the switch model. By default, this column is hidden. It can be selected by clicking the Settings button.
Switch Version	Displays the switch image version. By default, this column is hidden. It can be selected by clicking the Settings button.
Exporter ID	Displays the exporter ID that is configured on the switch as part of the flow analytics configuration.

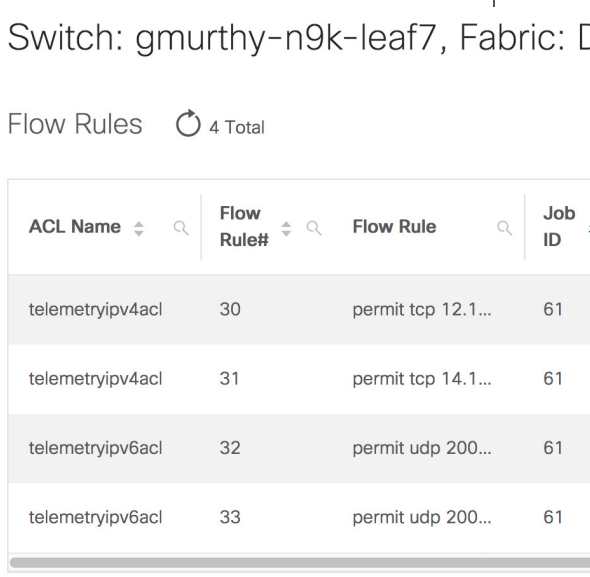
Field	Description
Receiver IP Port	Displays the comma-separated list of receiver IP addresses and ports assigned to a switch to transport flow telemetry data. The assigned IP addresses and ports will be that of the corresponding receiver microservices that are running in the NIR application and listening on the in-band network.
Expected Config	On clicking, it displays the expected configuration for the switch in a pop-up window. In case of an error, the reason for the error is displayed in the output.



Field	Description
Overall Status	

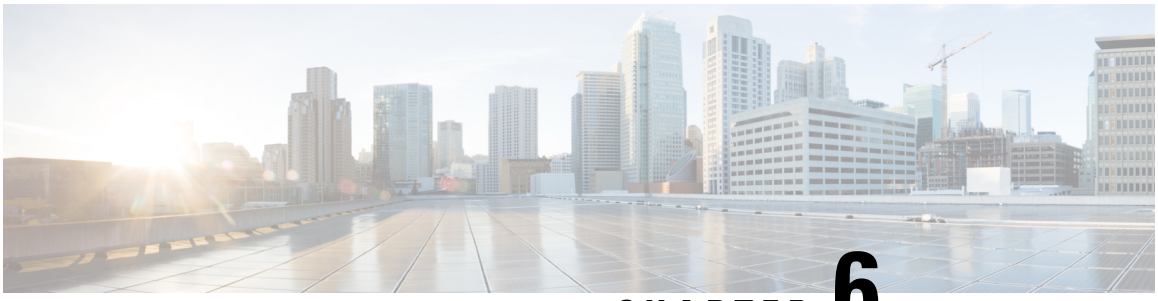
Field	Description
	The flow telemetry configuration involves 2 components namely the Flow telemetry setup and Flow ACL configurations. The overall status column displays the summary of both these statuses. The following statuses are displayed: **MONITOR**: Implies that the switch in the fabric was configured as "Monitored" in the NIR app. In this case, it is your responsibility to configure these switches manually with the telemetry configurations as displayed in the Expected Config column. **PROCESSING**: This indicates that the switch belonging to the fabric was configured as "Managed" in the NIR app. In this case, the telemetry manager will configure the switches and when configuration is in progress, it is displayed as "PROCESSING". **SUCCESS**: This indicates that the switches were successfully configured. **PARTIAL SUCCESS**: This indicates that some of the telemetry configurations could not be pushed to the switches. The Status Reason column will indicate the failure reason. **FAILED**: This indicates that the DCNM job failed to configure the switches. It could happen that some configuration did get pushed to the switches while some did not, in that case also DCNM marks the whole job as Failed. The Status Reason column will indicate the failure reason. You can filter the switches based on a particular status using the search option (or) you can sort the switches based on the status.

Field	Description
	
FT Setup Status	Displays the Flow telemetry setup status. If this shows **Failed**, it indicated that the flow analytics could not be enabled on the switches correctly and hence, the flow data cannot be exported from the switches.
Flow Rules Status (or) Flow ACL Status	Displays the Flow ACL configuration status in a color-coded format. The flow rules status count is divided into 3 categories: • Green (Success): Number of flow rules (ACEs) that got configured successfully. • Yellow (Pending): Number of flow rules (ACEs) that are pending to be configured. • Red (Failed): Number of flow rules (ACEs) that could not be configured.
Status Reason	Displays the failure reasons for the flow telemetry configuration (or) other information.

Field	Description
Flow Rules	Displays the following flow rule details: • **ACL Name**: The name of the access-list as configured on the switch. Only 2 ACLs get created namely telemetryipv4acl for IPv4 and telemetryipv6acl for IPv6. • **Flow Rule#**: This is the ACE rule number as configured within a particular ACL. • **Flow Rule**: This is the ACE rule that indicates the flow details like the protocol, source IP, source port, destination IP, destination port that should be exported. • **Job ID**: This is the DCNM telemetry job id that was used to configure the flow rules on the switch. • **Status**: The status of the job. • **Reason**: The status reason of the job. In case the job failed, it displays the failure reason of that job. If successful, it may show compliance and deployment successful in the case of Lan Fabric deployments. 

Note In case of MONITOR mode, you can configure flow telemetry on the switches using the following API that is available at https://<dcnm-ip>/api-docs: /telemetry/switches/{serialNumber}/flow-analytics-config -> where serialNumber is the switch serial number as a string.

The Health table data gets refreshed every 70 seconds automatically. It can be manually refreshed by clicking the Refresh icon.



CHAPTER 6

Media Controller

This section describes the Cisco DCNM Web Client UI **Media Controller** tab.

Note

- From Cisco DCNM Release 11.1(1), only a user with the network-admin role can configure a host or flow policy, and global configuration settings.
- IPFM maintains the last known monitored state of switches before they stop communicating. If switch doesn't report in 2 minutes, it will be marked as **Out Of Sync**. Check the sync status and the last sync timestamp by clicking **Telemetry Switch Sync Status** link on the respective monitoring page, for example, **Media Controller / Flow / Flow Status**.

To bring up the devices from the basic configuration using POAP, you must define the templates and publish the POAP definition through Cisco DCNM **Web Client > Configure > Deploy > POAP Definitions**. For more information, see the *POAP Launchpad* section.

Note Specific POAP templates for Leaf and Spine for the Media Controller deployment are packaged with the Cisco DCNM Software.

If you have configured the Cisco DCNM server in Media Controller mode and performed the procedure that is mentioned in the "POAP Launchpad" section, you will be able to see the Media Controller templates. Cisco DCNM Web Client allows you to choose the required templates, edit them as required, and publish the POAP definition.

For information about the Media Controller APIs, see the Cisco DCNM Media Controller API reference on Cisco DevNet.

You can use the DCNM media controller deployment for only monitoring purposes and not as a policy manager. For more information, see *DCNM Read-Only Mode for Media Controller*.

NX-OS Streaming Telemetry and DCNM

Using streaming telemetry, NBM process on the switch informs DCNM its state using which DCNM is able to show discovered hosts and flows across the IP fabric. The POAP and `pmn_telemetry_snmp` CLI template, which are packaged in DCNM, generate the necessary telemetry configuration on the switch. An example of the generated configuration is as shown in the following sample:

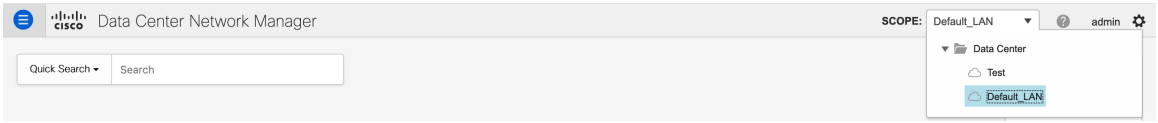
```
telemetry
  destination-profile
    use-vrf management
  destination-group 200
    ip address <dcnm-ip> port 50051 protocol gRPC encoding GPB
  destination-group 1500
  sensor-group 200
    data-source DME
    path sys/nbm/show/appliedpolicies depth unbounded
    path sys/nbm/show/stats depth unbounded
  sensor-group 201
    data-source DME
    path sys/nbm/show/flows depth 0 query-condition
    rsp-subtree-filter=eq(nbmNbmFlow.bucket,"1")&rsp-subtree=full
  sensor-group 202
    data-source DME
    path sys/nbm/show/flows depth 0 query-condition
    rsp-subtree-filter=eq(nbmNbmFlow.bucket,"2")&rsp-subtree=full
  sensor-group 203
    data-source DME
    path sys/nbm/show/flows depth 0 query-condition
    rsp-subtree-filter=eq(nbmNbmFlow.bucket,"3")&rsp-subtree=full
  sensor-group 204
    data-source DME
    path sys/nbm/show/flows depth 0 query-condition
    rsp-subtree-filter=eq(nbmNbmFlow.bucket,"4")&rsp-subtree=full
  sensor-group 205
    data-source DME
    path sys/nbm/show/endpoints depth unbounded
  sensor-group 300
    data-source NX-API
    path "show ptp brief"
    path "show ptp parent"
  sensor-group 301
    data-source NX-API
    path "show ptp corrections"
  sensor-group 500
    data-source NX-API
    path "show flow rtp details" depth 0
    path "show flow rtp errors active" depth 0
    path "show flow rtp errors history" depth 0
  subscription 201
    dst-grp 200
    snsr-grp 200 sample-interval 60000
    snsr-grp 201 sample-interval 30000
    snsr-grp 205 sample-interval 30000
  subscription 202
    dst-grp 200
    snsr-grp 202 sample-interval 30000
  subscription 203
    dst-grp 200
    snsr-grp 203 sample-interval 30000
  subscription 204
    dst-grp 200
    snsr-grp 204 sample-interval 30000
  subscription 300
    dst-grp 200
    snsr-grp 300 sample-interval 30000
    snsr-grp 301 sample-interval 30000
  subscription 500
    dst-grp 200
    snsr-grp 500 sample-interval 30000
```

Scope in Media Controller

The switch groups that you created in the **Administration** > **DCNM Server** > **Switch Groups** window are listed under the **SCOPE** drop-down list.

The **SCOPE** drop-down list is applicable for all the windows under **Media Controller** except the **Events** window.

For example, when you search in the **Topology** window, the search is effective only for the switch group that has been selected in the **SCOPE** drop-down list.



Similarly, the operations for Host, Flow, RTP Flow Monitor, and Global Config windows are effective only for the devices under the switch group selected in the **SCOPE** drop-down list.

The switch groups are separated from one another. For example, you can create a host alias with the same name and IP address for two different switch groups. For more information, see *Managing Switch Groups*.

Note If you select **Data Center** from the **SCOPE** drop-down list, you will see a pop-up window saying that Data Center is not supported.

- Topology, on page 149
- Host, on page 150
- Flow, on page 164
- RTP, on page 180
- Global, on page 184
- Config, on page 185
- DCNM Read-Only Mode for Media Controller, on page 193

Topology

You can view the Media Controller topology on the **Web UI** > **Media Controller** > **Topology** page. This topology is specific to the operations performed by DCNM as a Media Controller.

Note

- If you remove a device from the Inventory, the Policy deployment status for that switch is removed. However, clear the policy configuration on the switch also.
- After moving a cable from one port to another port, the old link is retained in the **Topology** window, and it's shown in the red color indicating that the link is down. The port movements aren't updated in the **Topology** window. Rediscover the switch for the updated ports to be displayed in DCNM.

Quick Search

Enter the search string to highlight relevant devices.

The following fields are available to search on: **switch or hostname**, **switch or host IP address**, **switch MAC**, and **switch serial number**.

Multicast Group

Right-click (or press Return Key) in the field. A list of multicast addresses are displayed. You can choose the multicast IP address for which you need to view the topology.

The devices under this multicast IP address, and links to spine and leaf are highlighted. The dotted moving lines depict the flow of traffic in the Media Controller topology.

You can search or filter based on flow alias name in the Topology. When you search for Multicast Group, you can search using the IP address or flow alias name.

Host

The Host menu includes the following submenus:

Discovered Host

You can view all the hosts that are populated through telemetry on this screen. After the switches are discovered, all the switches in the fabric will push data to the DCNM server at regular intervals using telemetry. Cisco DCNM server displays the received Events and Flow statistics for each active flow.

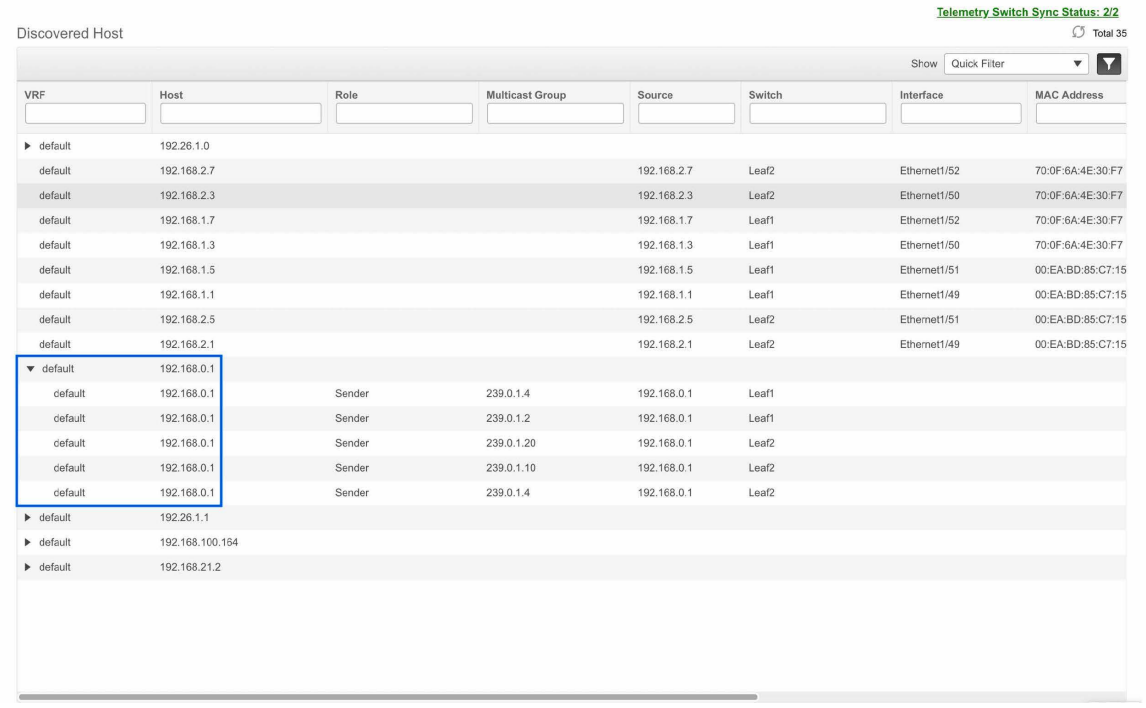
The following table describes the fields that appear on this page. Click the table header to sort the entries in alphabetical order of that parameter.

Table 23: Discovered Host Table Fields and Description

Field	Description
VRF	Specifies the VRF instance.
Host Name	Specifies the configured Host Alias for the host IP address. The Host IP is displayed if the Host Alias is not configured.
Role	Specifies the role of the host device. The role of the host can be one of the following: • Sender • External Sender • Dynamic Receiver • External Receiver • Static Receiver
Multicast Group	Specifies the multicast address of the flow in which the host participates.

Field	Description
Source	Specifies the source of the flow which the discovered host participates in.
Switch	Specifies the name of the switch.
Interface	Specifies the interface to which the host is connected to on the sender or receiver switch.
MAC Address	Specifies the MAC address of a physical host, if the switch has ARP entry for that host).
DCNM Discovered Time	Specifies the date and time at which the switch discovered the host.
Fault Reason	Specifies the failure reason for the flow that the discovered host has participates in.

Starting from Cisco DCNM Release 11.3(1), multiple entries of the same host are grouped together as an expandable row. Click the arrow icon to expand a specific row or collapse multiple rows into a single row.



Host Alias

Cisco DCNM allows you to create host aliases for Media Controller sender and receiver hosts. The active multicast traffic transmitting and receiving devices are termed as hosts. Beginning with Cisco DCNM Release 11.0(1), you can add a host-alias name to your sender and receiver hosts, to help you to identify the hosts by a name. You can also import many Host Alias to Cisco DCNM Media Controller.

The following table describes the fields that appear on this page.

Table 24: Host Alias Table Field and Description

Field	Description
Host Alias	Specifies the host name that is configured to identify the host.
IP Address	Specifies the IP address of the host connecting to the switch, which you want to refer with an alias name.
Last Updated At	Specifies the date and time at which the host alias was last updated.

This section contains the following:

Add Host Alias

Perform the following task to add new host aliases to devices in the fabric discovered by Cisco DCNM.

Procedure

Step 1 Choose **Media Controller > Host > Host Alias**, click **Add**.

Step 2 In the Add/Edit Host Alias window, enter the following:

- **Host Name—**Enter a fully qualified unified hostname for the identification.
- **IP Address—**Enter the IP address of the host that is the part of a flow.

Note You can also create host alias before a host sends any data to its directly connected sender or receiver leaf .

Step 3 Click **Save** to apply the changes.

Click **Cancel** to discard the host alias.

The new host alias is shown in the table on the **Host Alias** window.

Edit Host Alias

Perform the following task to edit the host alias.

Procedure

Step 1 Choose **Media Controller > Host > Host Alias**, select the check box next to the Host Alias that you need to modify.

Step 2 In the **Add/Edit Host Alias** window, enter the following:

- **Host Name—**Enter a fully qualified unified hostname for the identification.

- **IP Address**—Enter the IP address of the host that is the part of a flow.

Step 3 Click **Save** to apply the changes.

Click **Cancel** to discard the host alias.

The modified host alias is shown in the table on the **Host Alias** window.

Delete Host Alias

Perform the following task to delete the host alias.

Procedure

Step 1 Choose **Media Controller** > **Host** > **Host Alias**, select the check box next to the Host Alias that you want to delete.

You can select multiple Host Alias entries to be deleted at the same instance.

Step 2 Click **Delete**.

Step 3 On the confirmation window, click **OK** to delete the Host Alias.

Click **Cancel** to retain the host alias.

Import Host Alias

Perform the following task to import host aliases for devices in the fabric.

Procedure

Step 1 Choose **Media Controller** > **Host** > **Host Alias**, click **Import** icon.

Step 2 Browse the directory and select the CSV file, which contains the Host IP address and corresponding unique hostname information.

Step 3 Click **Open**.

The host aliases are imported and displayed on the Host Alias table.

Export Host Alias

Perform the following task to export host aliases for devices in the fabric.

Procedure

Step 1 Choose **Media Controller** > **Host** > **Host Alias**, click **Export** icon.

A notification window appears.

Step 2 Select a location on your local system directory to store the Host Aliases configuration from DCNM and click **OK**.

The host alias configuration file is exported to your local directory. The filename is appended with the date and time at which the file was exported. The format of the exported file is `.csv`.

Host Policies

You can add policies to the host devices. Navigate to **Media Controller > Host > Host Policies** to configure the host policies.



Note Switches must be deployed with default host policies. You can edit the default host policies to permit or deny. From the Deployment drop-down list, select **Deploy Selected Policies** to deploy the default policies to the switches.You can also deploy all the default policies to all the managed switches by selecting **Deploy All Default Policies** even without selecting any default policies.

By default, the sequence numbers for policies are auto-generated by DCNM and Multicast mask/prefix is taken as /32. The server property **pmn.hostpolicy.multicast-ranges.enabled** under **Administration > DCNM Server > Server Properties** must be set to '**true**' for the user to be able to provide sequence numbers and multicast mask/prefix. When the server property is set to **True**, the fields to enter the sequence number and the multicast mask/prefix is available in the **Media Controller > Host > Host Policies > Add** and **Media Controller > Host > Host Policies > Edit** pages.

The default host policies must be deployed successfully to the switch before you deploy the custom host policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add, edit, import, or deploy custom policies.



Note When a user logs in to DCNM with a network operator role, all the buttons or options to add, delete, modify, import, export, or deploy policies are disabled. This user can only view policies, and deployment status or history.

The following table describes the fields that appear on this page.

Table 25: Host Policies Operations

Field	Description
Add	Allows you to add a new host policy.
Edit	Allows you to view or edit the selected host policy parameters.

Field	Description
Delete	Allows you to delete the user-defined host policy. **Note** • Undeploy policies from all switches before deleting them from DCNM. • You can undeploy the default policy, but you cannot delete the default policy. You can delete and undeploy only the custom policies. • When you undeploy the default policies, All Default Policies will be reset to have default permission (Allow).
Delete All	Allows you to delete all custom policies without selecting any policy check box. **Note** • Undeploy policies from all switches before deleting them from DCNM. • You can undeploy the default policy, but you cannot delete the default policy. You can delete and undeploy only the custom policies.
Import	Allows you to import host policies from a CSV file to DCNM. **Note** After import, all policies imported from a CSV file are applied to all managed switches automatically.
Export	Allows you to export host policies from DCNM to a CSV file.

Field	Description
Deployment	

Field	Description

	From the Deployment drop-down list, select an appropriate value.
	• Deploy
	  • Selected Policies—Select this option to deploy selected policies to the switch.
	  • All Default Policies—Select this option to deploy all default policies to the switch.
	  • All Custom Policies—Select this option to deploy all the user-defined policies.
	• Undeploy
	  • Selected Policies—Select this option to undeploy the selected policies.
	  • All Default Policies—Select this option to undeploy the default policies.
	  • All Custom Policies—Select this option to undeploy all the user-defined policies.
	• Redo All Failed Policies—Select this option to deploy all failed policies.
	  All the deployments that failed on switches previously will be deployed again to only those switches. All the undeployments that failed on switches previously will be undeployed again from only those switches.
	• Deployment History—Select one policy from the drop-down list. Select this option to view the deployment history of the selected policy.
	  Deployment History shows the following fields.
	  • Policy Name—Displays the selected policy name.
	  • Switch Name—Specifies the name of the switch that the policy was deployed to.
	  • Deployment Status—Displays the status of deployment. It shows if the deployment was Success or Failed.
	  • Action—Specifies the action that is performed on the switch for that host policy. **Create** implies that the policy has been deployed on the switch. **Delete** implies that the policy has been undeployed from the switch.
	  • Deployment Date/Time—Specifies the date and time at which the host policy was last updated. The format is *Day MMM DD YYYY HH:MM:SS Timezone*.
	  • Failed Reason—Species why the policy was not

Field	Description
	successfully deployed.

Table 26: Host Policies Table Field and Description

Field	Description
Policy Name	Specifies the policy name for the host, as defined by the user.
Host Name	Specifies the host ID.
Receiver IP	Specifies the IP address of the receiving device.
Sender IP	Specifies the IP Address of the transmitting device.
Multicast IP	Specifies the multicast IP address for the host.
Sender IP	Specifies the IP Address of the sender.
Host Role	Specifies the host device role. The host device role is either one of the following: • Sender • Receiver-External • Receiver-Local
Operation	Specifies if the operation of the host policy. The policy has the following operations: • Permit • Deny
Sequence #	Specifies the sequence number of the custom policy when the multicast range is selected.
Deployment Action	Specifies the action performed on the switch for that host policy. • **Create—**The policy is deployed on the switch. • **Delete—**The policy is undeployed from the switch.
Deployment Status	Specifies if the deployment is successful, failed or the policy is not deployed.
Last Updated	Specifies the date and time at which the host policy was last updated. The format is `Day MMM DD YYYY HH:MM:SS Timezone`.

This section contains the following:

Add Host Policy

By default, the sequence number for policies is auto-generated by DCNM, and Multicast mask/prefix is /32 by default. The server property **pmn.hostpolicy.multicast-ranges.enabled** under **Administration > DCNM Server > Server Properties** must be set to '**true**' for the user to be able to provide sequence numbers and multicast mask/prefix. When the server property is set to **true**, the fields to enter the sequence number and the multicast mask/prefix are available in the **Media Controller > Host > Host Policies > Add** and **Media Controller > Host > Host Policies > Edit** windows.

The default host policies must be deployed successfully to the switch before you deploy the custom host policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add custom policies.

To add Host policy from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Host > Host Policies**.

The **Host Policies** window is displayed.

Step 2 Click the **Add** icon.

Step 3 In the Add Host Policy window, specify the parameters in the following fields.

- **Policy Name**: Specifies a unique policy name for the host policy.
- **Host Role**: Specifies the host as a multicast sender or receiver. Select one of the following:
  - Sender
  - Receiver-Local
  - Receiver-External
- **Host Name**: Specifies the host to which the policy is applied. If a destination host is detected, you can choose the hostname from the drop-down list.

  Note Do not select hosts that are discovered as remote receivers to create receiver or sender host policies. However, hosts that are discovered as remote senders can be used for creating sender host policies.
- **Sender IP**: Specifies the IP address of the Sender host. Note that you can specify wildcard for this IP address by specifying the * (asterisk) symbol or 0.0.0.0 in this field.
- **Receiver IP**: Specifies the IP address of the receiver host. This field is visible and is applicable only if the Host Role is set to **Receiver-Local**. Note that you can specify wildcard for this IP address by specifying the * (asterisk) symbol or 0.0.0.0 in this field.

  Note When **Receiver IP** in a receiver host policy is a wildcard (* or 0.0.0.0), **Sender IP** also has to be a wildcard (* or 0.0.0.0).
- **Multicast**: Specifies the multicast IP Address for the host policy. Note that you can specify wildcard for this IP address by specifying the * (asterisk) symbol in this field. This will translate to 224.0.0.0/4. If you specify a wildcard IP address for **Sender IP** and **Receiver IP** fields, the Multicast Group is always required, that is, you cannot specify multicast as * or 0.0.0.0.

- **Allow/Deny**: Click the radio button to choose, if the policy must **Allow** or **Deny** the traffic flow.

Step 4 Click **Save & Deploy** to configure and deploy the Policy.

Click **Cancel** to discard the new policy.

Edit Host Policy

The default host policies must be deployed successfully to the switch before you deploy the custom host policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you edit custom policies.

To edit host policy from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller** > **Host** > **Host Policies**.

The **Host Policies** window is displayed.

Step 2 Check the check box next to the host policy name, that you need to edit.

Step 3 Click **Edit** Host policy icon.

Step 4 In the Edit Host Policy window, edit to specify if the policy will **Allow** or **Deny** traffic.

Note The changes made to Host Policy are applied immediately. If the policy is already applied to any device, the changes may impact the existing flows.

Step 5 Click **Save & Deploy** to configure and deploy the Policy.

Click **Cancel** to discard the changes.

Delete Host Policy

To delete host policy from the Cisco DCNM Web UI, perform the following steps:



Note You can delete only user-defined Host Policies.

Procedure

Step 1 Choose **Media Controller** > **Host** > **Host Policies**.

The **Host Policies** window is displayed.

Step 2 Check the check box next to the host policy name, that you need to delete.

You can select more than one host policy to delete.

Step 3 Click **Delete** Host policy icon.

Click **Delete All** to delete all the policies at a single instance.

Step 4 In the delete notification, click **OK** to delete the host policy. Click **Cancel** to return to the Host Policies page.

Note Deleting a host policy from DCNM does not undeploy the policy from the switches on which it is deployed. It is highly recommended to undeploy the policy on the switches before deleting it from DCNM.

A Delete Host policy successful message appears at the bottom of the page.

Import Host Policy

The default host policies must be deployed successfully to the switch before you deploy the custom host policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add custom policies.

To import host policies from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller** > **Host** > **Host Policies**.

The **Host Policies** window is displayed.

Step 2 Click the **Import** host policy icon.

Step 3 Browse the directory and select the `.csv` format file which contains the Host Policy configuration information.

The policy will not be imported if the format in the `.csv` file is incorrect.

Step 4 Click **Open**.

The imported policies are automatically deployed to all the switches in the fabric.

Export Host Policy

To export host policies from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller** > **Host** > **Host Policies**.

The **Host Policies** window is displayed.

Step 2 Click the **Export** host policy icon.

A notification window appears.

Step 3 Select a location on your directory to store the Host Policy details file.

Step 4 Click **OK**.

The host policy file is exported to your local directory. The filename is appended with the date on which the file is exported. The format of the exported file is `.csv`.

Policy Deployment

Policies are automatically deployed to switches whenever they are added, edited, or imported. You can choose to undeploy or redeploy the policies, by choosing the appropriate actions in the **Deployment** drop-down list. The policies will not be deployed correctly if the device is rebooting while the policy was deployed. In such case, the Failed message appears in the Status column in the table below.

The default policies must be deployed successfully to the switch before you deploy the custom policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add custom policies.

Deploy Selected Policies

This option allows you to deploy only selected policies to the devices. You can deploy other policies when required.

Select one or more check boxes next to the policy name. Select this option to deploy selected policies to the switch.

Deploy All Custom Policies

This option allows you to deploy all the custom or user-defined policies to the switch. The policies are deployed even if the switch is rebooting. In such case, the deployment fails and a status message Failed appears in the table below.

Select this option to deploy all the user-defined policies at a single instance.

Undeploy Selected Custom Policies

Select one or more check boxes next to the policy name. Select this option from the drop-down list to undeploy the selected policies.

Undeploy All Custom Policies

This option allows you to undeploy all the custom or user-defined policies in a single instance.

Note From Cisco DCNM Release 11.2(1), you can deploy and undeploy default policies also.

Redo All Failed Custom Policies

The deployment of policies may fail due to various reasons. This option allows you to deploy all failed user-defined policies.

All the deployments that failed previously are deployed again only to those switches. All the undeployments failed previously are redeployed from only those switches.

Deployment History

This option allows you to view the deployment history of the policy.

The policy name is shown in the Policy Name field. From the drop-down list, choose the switch on which this policy was deployed.

The deployment history of the selected policy for the switch appears in the table below.

Deployment History table shows the following fields.

Table 27: Policy Deployment History Table Field and Descriptions

Field	Description
Deployment Status	Displays the deployment status of the policy. It shows if the deployment was Success or Failed.
Deployment Action	Specifies the action that is performed on the switch for that policy. **Create**: The policy is deployed on the switch. **Delete**: The policy is undeployed from the switch.
Deployment Date/Time	Specifies the date and time at which the host policy was last updated. The format is *Day MMM DD YYYY HH:MM:SS Timezone*.
Failed Reason	Species why the policy was not successfully deployed.

Applied Host Polices

Beginning from Cisco DCNM Release 11, you can view the policies that you have applied in the entire network. On the Cisco DCNM Web UI, navigate to **Media Controller > Host > Applied Host Policies** to view the various policies.

The table displays default PIM policy, local receiver policy, and sender policy. Media Controller will not display user-defined PIM Policies or Receiver External Policies.

The following table describes the fields that appear on this page.

Table 28: Field and Description on the Applied Host Policies

Column Name	Description
Policy Name	Specifies the name of the policy applied.
Host Role	Specifies the role of the host. The host device role is either one of the following: • PIM • Sender • Receiver

Column Name	Description
Switch	Specifies the name of the switch to which the policy is applied.
Interface	Specifies the interface to which the policy is applied.
Active	Specifies if the policy is active or not.
Time Stamp	Specifies the date and time at which the policy was created\deployed. The format is Day, MMM DD YYYY HH:MM:SS (Timezone).

Flow

The Flow menu includes the following submenus:

Flow Status

Cisco DCNM allows you to view the flow status pictorially and statistically. The flow status is available on **Media Controller > Flow > Flow Status**.

Fields and Descriptions

The following table describes the fields that appear on the Active tab.

Table 29: Active Tab

Field	Description
Show Chart	Click Show Chart icon to view the graphical representation of the Flow Status. **Note** The data refers to the sender leaf when the sender starts broadcasting. See the receiver start time in the flow status table to find when the receiver started getting data. Click the **Show** drop-down list to view the flow status information in one of the following formats—Chart, Table, or Chart and Table. Click **Chart Type** icon to view the various chart types. Select a chart type to view the flow status information that is depicted in that chart format. You can choose a chart option to see filled patterns or data markers. Click **Actions** icon to print the report or excel chart information to your local directory.

Field	Description
Multicast IP	Specifies the multicast IP address for the flow. **Note** You can click the wave link next to the Multicast IP address to view the pictorial representation of flow statistics.
Flow Alias	Specifies the name of the Flow Alias.
Policed	Specifies whether a flow is policed or not policed.
Sender	Specifies the IP Address or the Host alias of the sender for the multicast group.
Receiver	Specifies the IP Address or the Host alias of the receiver joining the group.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.
Sender Switch	Specifies if the Sender switch is a leaf or spine.
Sender Interface	Specifies the interface to which the sender is connected to.
Receiver Switch	Specifies if the Receiver switch is a leaf or spine.
Receiver Interface	Specifies the interface to which the receiver is connected to.
QOS/DSCP	Specifies the Switch-defined QoS Policy.
Flow Link State	Specifies the state of the flow link. Click **active** link to view the network diagram of the Sender and Receiver. The dotted line displays the direction of the flow of traffic. You can hover over the nodes to view information. The table on the right side shows information about the Sender and Receiver.
Policy ID	Specifies the policy ID applied to the multicast IP.
Sender Start Time	Displays the time from when the sender joined.
Receiver Join Time	Specifies the time at which the receiver joined.

The following table describes the fields that appear on the Inactive tab.

Table 30: Inactive Tab

Field	Description
Show Chart	Click Show Chart icon to view the graphical representation of the Flow Status. **Note** The data refers to the sender leaf when the sender starts broadcasting. Please see the receiver start time in the flow status table to find when the receiver started getting data. Click the **Show** drop-down list to view the flow status information in one of the following formats—Chart, Table, or Chart and Table. Click **Chart Type** icon to view the various chart types. Select a chart type to view the flow status information that is depicted in that chart format. You can choose a chart option to see filled patterns or data markers. Click icon to print the report or excel chart information to your local directory.
Multicast IP	Specifies the multicast IP address of the flow.
Flow Alias	Specifies the name of the Flow Alias.
Policed	Specifies whether a flow is policed or not policed.
Sender	Specifies the IP Address or the Host alias of the sender for the multicast groups.
Receiver	Specifies the IP Address or the Host alias of the receiver.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.
QoS/DSCP	Specifies the Switch-defined QoS Policy.
Policy ID	Specifies the policy ID applied to the multicast IP.
Sender Start Time	Specifies the time at which the sender joined.
Receiver Join Time	Specifies the time at which the receiver joined.

Field	Description
Fault Reason	Specifies reason for the inactive flow. Cisco DCNM determines the inactive flow if both the sender and receiver mroute exists with any of the following combinations. • Receiver IIF is null • Receiver OIF is null • Sender IIF is null • Sender OIF is null In this scenario, the switch won't have any fault reason. Therefore, there's no fault reason for such inactive flows.

The following table describes the fields that appear on the Sender Only tab.

Table 31: Sender Only Tab

Field	Description
Multicast IP	Specifies the multicast IP address for the flow.
Flow Alias	Specifies the name of the Flow Alias.
Policed	Specifies whether a flow is policed or not policed.
Sender	Specifies the name of the sender.
Sender Switch	Specifies the IP address of the sender switch.
Sender Ingress Interface	Specifies the name of the sender ingress interface.
Flow Link State	Specifies the flow link state, if it is allow or deny.
Policy ID	Specifies the policy ID applied to the multicast IP.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.
Sender Start Time	Displays the time from when the sender switch is transmitting information.

The following table describes the fields that appear on the Receiver Only tab.

Table 32: Receiver Only Tab

Field	Description
Multicast IP	Specifies the multicast IP address for the flow.
Flow Alias	Specifies the name of the Flow Alias.

Field	Description
Name	Specifies the receiver ID. If the multicast receiver is remote, the **Remote** label can be seen next to its name.
Receiver Interface	Specifies the name of the destination switch interface.
Receiver Switch	Specifies the IP address of the receiver switch.
Source Specific Sender	Specifies the IP address of the multicast sender.
Flow Link State	Specifies the flow link state, if it's allow or deny.
Policy ID	Specifies the policy ID applied to the multicast IP.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.
Receiver Join Time	Specifies the time at which the receiver joined.

Click the **Show** drop-down list in the statistical representation area to display the statistical data in various formats.

Click the arrow to export the statistical data. You can export it in `.csv` or `.pdf` formats.

Note Cisco DCNM holds the Flow statistics values in the DCNM server internal memory. Therefore, after a DCNM Restart or HA switch over, the Flow statistics won't show previously collected values. However, you can see the Flow statistics that are collected after the server Restart or HA switch over.

If the new flow joins before the uplinks between the switches that are detected in DCNM, a message BW_UNAVAIL appears. This is resolved after the uplinks between the switches are detected by DCNM after discovery of the devices.

Flow Alias

Using the Flow Alias feature, you can specify names for multicast groups. The multicast IP addresses are difficult to remember, thus by assigning a name to the multicast IP address, you can search and add policies based on the name.

You can configure a flow alias on **Media Controller > Flow > Flow Alias**.

The following table describes the fields that appear on this page.

Table 33: Flow Alias Table Field and Description

Field	Description
Flow Alias	Specifies the name of the Flow Alias.
Multicast IP Address	Specifies the multicast IP address for the traffic.
Description	Description added to the Flow Alias.

Field	Description
Last Updated at	Specifies the date on which the flow alias was last updated.

This section contains the following:

Add Flow Alias

To add flow alias from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Alias**.

The **Flow Alias** window is displayed.

Step 2 Click the **Add** Flow Alias icon.

Step 3 In the **Add Flow Alias** window, specify the parameters in the following fields.

- **Flow Name**: Specifies a unique flow alias name.
- **Multicast IP Address**: Specifies the multicast IP Address for the flow alias.
- **Description**: Specifies the description that you add for the flow alias.

Step 4 Click **Save** to save the flow alias.

Click **Cancel** to discard.

Edit Flow Alias

To edit a flow alias from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Alias**.

The **Flow Alias** window is displayed.

Step 2 Check the check box next to the flow alias name, that you need to edit.

Step 3 Click **Edit** Flow Alias icon.

Step 4 In the Edit Flow Alias window, edit the **Name**, **Multicast IP**, **Description** fields.

Step 5 Click **Save** to save the new configuration.

Click **Cancel** to discard the changes.

Delete Flow Alias

To delete flow alias from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Alias**.

The **Flow Alias** window is displayed.

Step 2 Check the check box next to the flow alias, that you need to delete.

You can select more than one flow alias to delete.

Step 3 Click **Delete** Flow Alias icon.

The flow alias is deleted.

Export Flow Alias

To export host alias from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Alias**.

The **Flow Alias** window is displayed.

Step 2 Click **Export** flow alias icon.

A notification window appears.

Step 3 Select a location on your directory to store the Alias details file.

Step 4 Click **OK**.

The flow alias file is exported to your local directory. The filename is appended with the date on which the file is exported. The format of the exported file is `.csv`.

Import Flow Alias

To import flow alias from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Alias**.

The **Flow Alias** window is displayed.

Step 2 Click **Import** flow alias icon.

Step 3 Browse the directory and select the file which contains the Flow Alias configuration information.

Step 4 Click **Open**.

The flow alias configuration is imported and displayed on the **Media Controller > Flow > Flow Alias** window, on the Cisco DCNM Web Client.

Flow Policies

You can configure the flow policies on **Media Controller > Flow > Flow Policies**.

The default policies are displayed on the Flow policy page. By default, the bandwidth of these policies is 0. You can configure the bandwidth such that any flow that matches the default flow policy will accordingly use the bandwidth and QOS/DSCP parameters. The policy is deployed to all the devices when you save the configuration.

The default flow policies must be deployed successfully to the switch before you deploy the custom flow policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add, edit, import, or deploy custom policies.

Note When you undeploy a default policy, it will be reset to default values, that is, Bandwidth:0gbps, DSCP:Best Effort, and Policer:Enabled.

Note When a user logs in to DCNM with a network operator role, all the buttons or options to add, delete, modify, import, export, or deploy policies are disabled. This user can only view policies, and deployment status or history.

The following table describes the fields that appear on this page.

Table 34: Flow Policies Operations

Field	Description
Add	Allows you to add a new flow policy.
Edit	Allows you to view or edit the selected flow policy parameters.
Delete	Allows you to delete the user-defined flow policy. **Note** • You cannot delete the default flow policies. • Undeploy policies from all switches before deleting them from DCNM.

Field	Description
Delete All	Allows you to delete all the flow policies at a single instance. **Note** Undeploy policies from all switches before deleting them from DCNM.
Import	Allows you to import flow policies from a CSV file. **Note** After import, all policies imported from a CSV file are applied to all managed switches automatically.
Export	Allows you to export flow policies to a CSV file.

Field	Description
Deployment	

Field	Description

	From the Deployment drop-down list, select an appropriate value.
	• Deploy
	  • Selected Policies—Select this option to deploy selected policies to the switch.
	  • All Default Policies—Select this option to deploy all default policies to the switch.
	  • All Custom Policies—Select this option to deploy all the user-defined policies.
	• Undeploy
	  • Selected Policies—Select this option to undeploy the selected policies.
	  • All Default Policies—Select this option to undeploy the default policies.
	  • All Custom Policies—Select this option to undeploy all the user-defined policies.
	• Redo All Failed Policies—Select this option to deploy all failed policies.
	  All the deployments that failed on switches previously will be deployed again to only those switches. All the undeployments that failed on switches previously will be undeployed again from only those switches.
	• Deployment History—Select one policy from the drop-down list. Select this option to view the deployment history of the selected policy.
	  Deployment History shows the following fields.
	  • Policy Name—Displays the selected policy name.
	  • Switch Name—Specifies the name of the switch that the policy was deployed to.
	  • Deployment Status—Displays the status of deployment. It shows if the deployment was Success or Failed.
	  • Specifies the action that is performed on the switch for that flow policy.
	  • **Create**—Implies that the policy has been deployed on the switch.

Field	Description
	• **Delete**—Implies that the policy has been undeployed from the switch. • Deployment Date/Time—Specifies the date and time at which the host policy was last updated. The format is *Day MMM DD YYYY HH:MM:SS Timezone*. • Failed Reason—Species why the policy was not successfully deployed.

Table 35: Flow Policies Table Field and Description

Field	Description
Policy Name	Specifies the flow policy name.
Multicast IP Range	Specifies the multicast IP address for the traffic.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.
QoS/DSCP	Specifies the Switch-defined QoS Policy.
Deployment Status	Specified if the flow policy is deployed successfully or failed.
Deployment Action	Specifies the action that is performed on the switch for that host policy. • **Create**—The policy is deployed on the switch. • **Delete**—The policy is undeployed from the switch.
In Use	Specifies if the flow policy is in use or not.
Policer	Specifies whether the policer for a flow policy is enabled or disabled. **Note** In adding or editing a flow policy, the default policer state is **Enabled**.
Last Updated	Specifies the date and time at which the flow policy was last updated. The format is `Day MMM DD YYYY HH:MM:SS Timezone`.

Note A new flow policy or an edited flow policy is effective only under the following circumstances.

- If the new flow matches the existing flow policy.
- If the flow expires and reforms, while the new policy is already added or edited, that matches with the flow policy.

This section contains the following:

Add Flow Policy

The default host policies must be deployed successfully to the switch before you deploy the custom host policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add custom policies.

To add flow policy from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Policies**.

The **Flow Policies** window is displayed.

Step 2 Click the **Add** Flow policy icon.

Step 3 In the Add Flow Policy window, specify the parameters in the following fields.

- **Policy Name**: Specifies a unique policy name for the flow policy.
- **Bandwidth**: Specifies the bandwidth that is allocated for the flow policy. Select of the radio buttons to choose **Gbps** or **Mbps**.

Step 4 From the **QoS/DSCP** drop-down list, choose an appropriate ENUM value.

Step 5 Click the **Policer** toggle switch to enable or disable policer for a flow. By default, the poilcer for a new flow policy is enabled.

Step 6 In the Multicast IP Range, enter the beginning IP and ending IP Address for the multicast range.

Click **Plus (+)** icon to add the multicast range to the policy.

Step 7 Click **Deploy** to deploy the new policy.

Click **Cancel** to discard the changes.

Edit Flow Policy

The default flow policies must be deployed successfully to the switch before you deploy the custom flow policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you edit custom policies.

To add flow policy from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Policies**.

The **Flow Policies** window is displayed.

Step 2 Check the check box next to the flow policy name, that you need to edit.

Step 3 Click **Edit** Flow policy icon.

Step 4 In the Edit Flow Policy window, edit the **Multicast IP**, **Bandwidth**, **QoS/DSCP** fields.

Step 5 Click the **Policer** toggle switch to enable or disable policer for a flow policy.

Step 6 Click **Deploy** to deploy the new policy.

Click **Cancel** to discard the changes.

Delete Flow Policy

To delete flow policy from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Policies**.

The **Flow Policies** window is displayed.

Step 2 Check the check box next to the flow policy name, that you need to delete.

You can select more than one flow policy to delete.

Note You cannot delete the default policies.

Step 3 Click **Delete** icon to delete the selected flow policy.

Click **Delete All** icon to delete all the flow policies at a single instance.

Import Flow Policy

The default flow policies must be deployed successfully to the switch before you deploy the custom flow policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you import custom policies.

To import flow policies from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Policies**.

The **Flow Policies** window is displayed.

Step 2 Click the **Import** flow policy icon.

Step 3 Browse the directory and select the file which contains the Flow Policy configuration information.

Step 4 Click **Open**.

The flow policy configuration is imported and displayed on the **Media Controller > Flow > Flow Policies** window, on the Cisco DCNM Web Client.

The imported policies are automatically deployed to all the switches in the fabric.

Export Flow Policy

To export host policies from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Policies**.

The **Flow Policies** window is displayed.

Step 2 Click the **Export** flow policy icon.

A notification window appears.

Step 3 Select a location on your directory to store the Flow Policy details file.

Step 4 Click **OK**.

The flow policy file is exported to your local directory. The filename is appended with the date on which the file is exported. The format of the exported file is `.csv`.

Policy Deployment

Policies are automatically deployed to switches whenever they are added, edited, or imported. You can choose to undeploy or redeploy the policies, by choosing the appropriate actions in the **Deployment** drop-down list. The policies will not be deployed correctly if the device is rebooting while the policy was deployed. In such case, the Failed message appears in the Status column in the table below.

The default policies must be deployed successfully to the switch before you deploy the custom policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add custom policies.

Deploy Selected Policies

This option allows you to deploy only selected policies to the devices. You can deploy other policies when required.

Select one or more check boxes next to the policy name. Select this option to deploy selected policies to the switch.

Deploy All Custom Policies

This option allows you to deploy all the custom or user-defined policies to the switch. The policies are deployed even if the switch is rebooting. In such case, the deployment fails and a status message Failed appears in the table below.

Select this option to deploy all the user-defined policies at a single instance.

Undeploy Selected Custom Policies

Select one or more check boxes next to the policy name. Select this option from the drop-down list to undeploy the selected policies.

Undeploy All Custom Policies

This option allows you to undeploy all the custom or user-defined policies in a single instance.



Note From Cisco DCNM Release 11.2(1), you can deploy and undeploy default policies also.

Redo All Failed Custom Policies

The deployment of policies may fail due to various reasons. This option allows you to deploy all failed user-defined policies.

All the deployments that failed previously are deployed again only to those switches. All the undeployments failed previously are redeployed from only those switches.

Deployment History

This option allows you to view the deployment history of the policy.

The policy name is shown in the Policy Name field. From the drop-down list, choose the switch on which this policy was deployed.

The deployment history of the selected policy for the switch appears in the table below.

Deployment History table shows the following fields.

Table 36: Policy Deployment History Table Field and Descriptions

Field	Description
Deployment Status	Displays the deployment status of the policy. It shows if the deployment was Success or Failed.
Deployment Action	Specifies the action that is performed on the switch for that policy. **Create**: The policy is deployed on the switch. **Delete**: The policy is undeployed from the switch.

Field	Description
Deployment Date/Time	Specifies the date and time at which the host policy was last updated. The format is *Day MMM DD YYYY HH:MM:SS Timezone*.
Failed Reason	Species why the policy was not successfully deployed.

RTP

The **RTP** menu includes the **RTP Flow Monitor** submenu.

RTP Flow Monitor

Cisco DCNM provides a view of all the active RTP stream. It also lists out active flows that have RTP drops and historical records for the same. For active media controller flow, DCNM provides RTP topology to pinpoint the loss in network.



Note You need to enable telemetry in the switches to view RTP Flow Monitor. For more information, refer your respective platform documentation.

To view **RTP Flow Monitor**, choose **Media Controller > RTP > RTP Flow Monitor**.

The RTP Flow monitor window has three tabs: **Active**, **Packet Drop**, and **Drop History**.

The description of the fields in these tabs are:

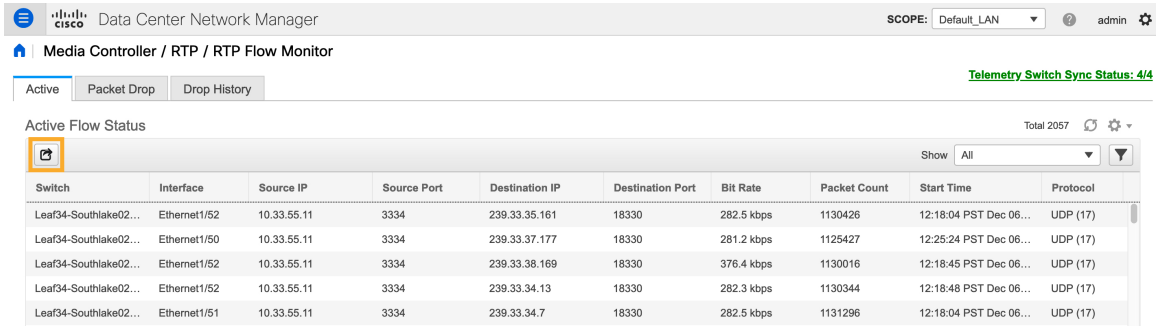
Field	Description
Switch	Specifies the name of the switch.
Interface	Specifies the interface from which the flows are detected.
Source IP	Specifies the source IP address of the flow.
Source Port	Specifies the source port of the flow.
Destination IP	Specifies the destination IP address of the flow.
Destination Port	Specifies the destination port of the flow.
Bit Rate	Specifies the bit rate of the flow, in bps, kbps, mbps, gbps, or tbp.
Packet Count	Specifies the number of packets in the flow.
Packet Loss	Specifies the number of lost packets.
Loss Start	Specifies the time at which the packet loss started.

Field	Description
Loss End	Specifies the time at which the packet loss stopped.
Start Time	Specifies the time at which the flow started.
Protocol	Specifies the protocol that is being used for the flow.

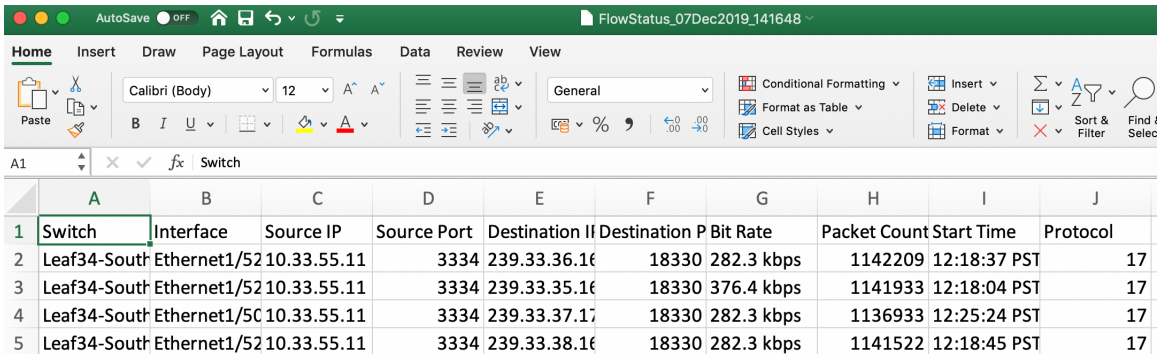
You can click the **Telemetry Switch Sync Status** link to check whether the switches are in sync. The **Sync Status** column displays the status of the switches.

Active

The **Active** tab displays the current active flows. You can also view these flows by navigating to **Media Controller > Flow > Flow Status**.

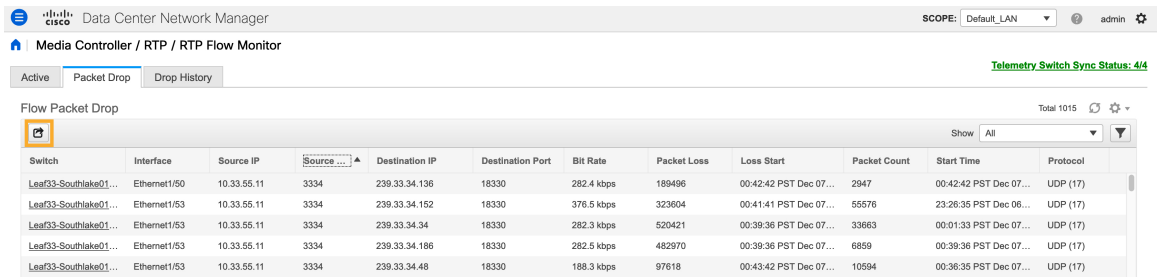


Click the **Export** icon at the top left of the table to export the Active Flow Status data in a .csv file.

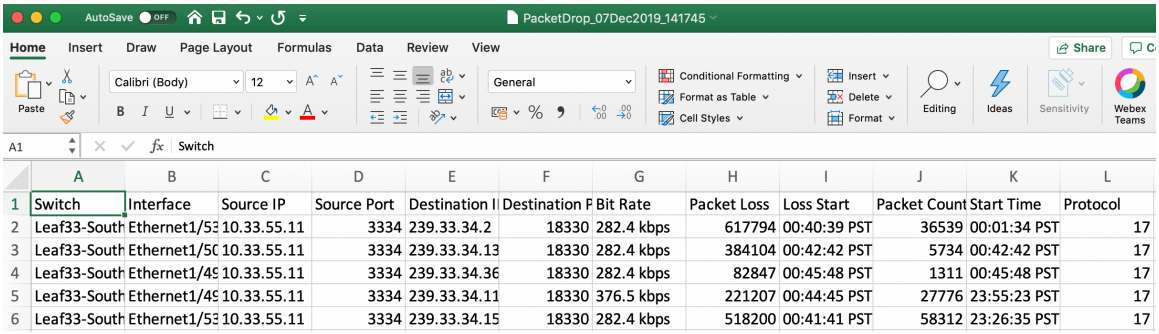


Packet Drop

The **Packet Drop** tab shows the packet drops for active flows.



Click the **Export** icon at the top left of the table to export the Packet Drop data in a .csv file.

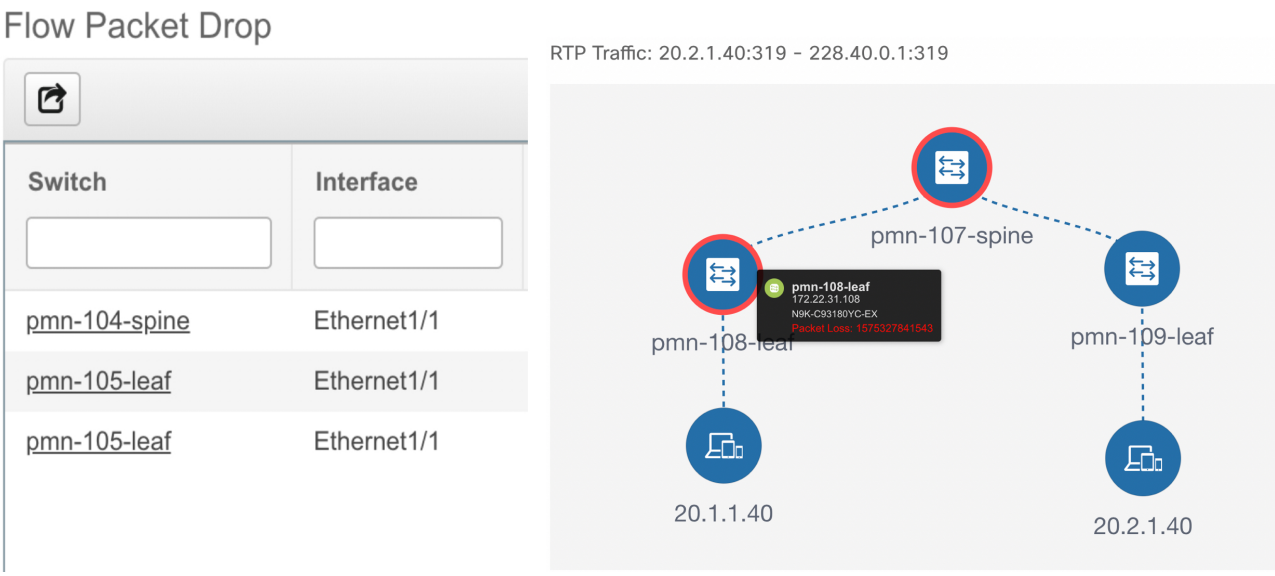


	A	B	C	D	E	F	G	H	I	J	K	L
1	Switch	Interface	Source IP	Source Port	Destination I	Destination P	Bit Rate	Packet Loss	Loss Start	Packet Count	Start Time	Protocol
2	Leaf33-South	Ethernet1/53	10.33.55.11	3334	239.33.34.2	18330	282.4 kbps	617794	00:40:39 PST	36539	00:01:34 PST	17
3	Leaf33-South	Ethernet1/50	10.33.55.11	3334	239.33.34.13	18330	282.4 kbps	384104	00:42:42 PST	5734	00:42:42 PST	17
4	Leaf33-South	Ethernet1/49	10.33.55.11	3334	239.33.34.36	18330	282.4 kbps	82847	00:45:48 PST	1311	00:45:48 PST	17
5	Leaf33-South	Ethernet1/49	10.33.55.11	3334	239.33.34.11	18330	376.5 kbps	221207	00:44:45 PST	27776	23:55:23 PST	17
6	Leaf33-South	Ethernet1/53	10.33.55.11	3334	239.33.34.15	18330	282.4 kbps	518200	00:41:41 PST	58312	23:26:35 PST	17

Flow Topology

The flow topology is displayed for the active flows that are displayed in the **Media Controller > Flow Status** window.

Click a switch link to display the end-to-end flow topology.



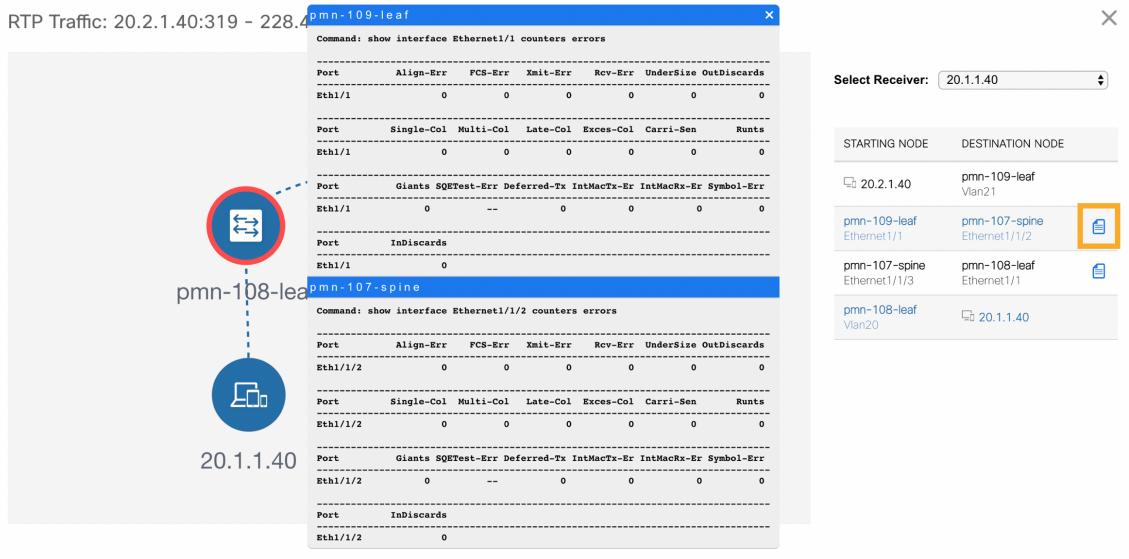
The flow topology displays the direction of the flows, that is, from sender to the receiver. If there are multiple receivers for a given flow, you can choose a receiver from the **Select Receiver** drop-down list.

The switches experiencing packet drops are circled in red.

Hover your cursor over a switch to display the following details:

- Name
- IP address
- Model
- Packet loss, if any

Click the **file** icon next to the links between the switches to view the interface counters errors for the interfaces connecting the two switches.

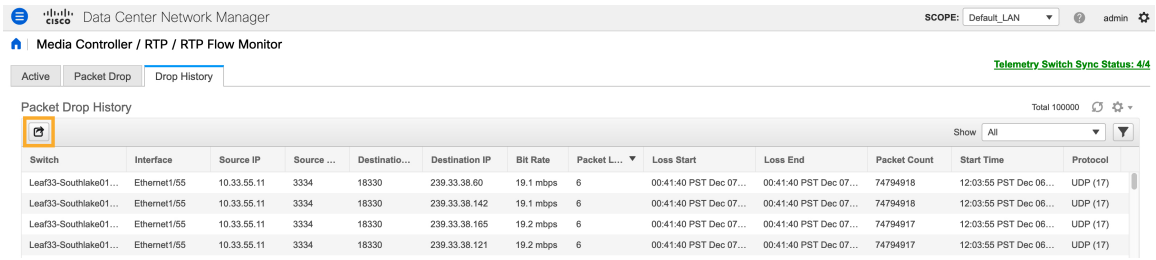


When you click the file icon, the **show interface <*interface name*> counters errors** command is run for the interface where the flow is participating between these switches, and the results are displayed in a pop-in.

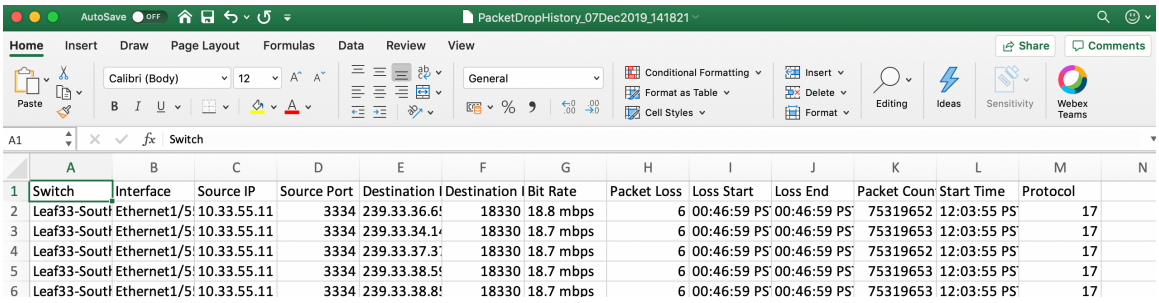
Drop History

When active RTP packet drop is not observed, records from the **Packet Drop** tab are moved to the **Drop History** tab. By default, the RTP drop history is maintained for 7 days. You can customize this setting by updating value for the **pmn.elasticsearch.history.days** property in the **Administration** > **DCNM Server** > **Server Properties** window.

Note The **Drop History** tab displays only the last 100,000 records at the maximum.



Click the **Export** icon at the top left of the table to export the Packet Drop History data in a .csv file.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Switch	Interface	Source IP	Source Port	Destination I	Destination I	Bit Rate	Packet Loss	Loss Start	Loss End	Packet Coun	Start Time	Protocol	
2	Leaf33-Soutl	Ethernet1/5	10.33.55.11	3334	239.33.36.6	18330	18.8 mbps	6	00:46:59 PS	00:46:59 PS	75319652	12:03:55 PS	17	
3	Leaf33-Soutl	Ethernet1/5	10.33.55.11	3334	239.33.34.1	18330	18.7 mbps	6	00:46:59 PS	00:46:59 PS	75319653	12:03:55 PS	17	
4	Leaf33-Soutl	Ethernet1/5	10.33.55.11	3334	239.33.37.3	18330	18.7 mbps	6	00:46:59 PS	00:46:59 PS	75319652	12:03:55 PS	17	
5	Leaf33-Soutl	Ethernet1/5	10.33.55.11	3334	239.33.38.5	18330	18.7 mbps	6	00:46:59 PS	00:46:59 PS	75319653	12:03:55 PS	17	
6	Leaf33-Soutl	Ethernet1/5	10.33.55.11	3334	239.33.38.8	18330	18.7 mbps	6	00:46:59 PS	00:46:59 PS	75319653	12:03:55 PS	17	

For information about the AMQP based notifications, see Cisco DCNM IP for Media Deployment - AMQP Notifications and for information about REST APIs, see Cisco DCNM API Reference Guide.

Global

The Global menu includes the following submenus:

Events

Cisco DCNM allows you to view and purge the various events between the Host and Flow. The Events are recorded on **Media Controller > Events**.

The PMN Events table is updated real-time.

The maximum stored PMN events and cleanup frequency can be specified via **pmn.rows.limit** and **pmn.delete.interval** respectively in the **Administration > DCNM Server > Server Properties** page.

The following table describes the fields that appear on this page.

Field	Description
Purge	Click to remove the old/unwanted events. **Note** If the DCNM server restarts, by default a maximum of 5000 event entries are retained for 6 hours. Click one of the radio buttons to choose the Purge options. • **Max # of Records**—Enter the maximum number of records to delete. • **# of Days**—Enter the number of days for which you need to delete the events. • **Delete all data from the previous date**—Specifies a date before which all the data is deleted. Click **Purge** to delete/retain PMN events information.
Category	Specifies if the event category.
Severity	Specifies the severity of the event.

Field	Description
Description	Specifies the description of the event. The sample description appears as: `Creating flow for FlowRequest:The flowRequest is for hostId:<<IP_Address>> hostInterface:<<Host_Int_ID>> mcastIp:<<Multicast IP>> Is sender role:false originating from switch:<<Host IP Address>>`
Impacted Flows	Specifies the impacted flows due to this event.
Last Update Time	Specifies the date and time at which the event was last modified. The format is *Day MMM DD YYYY HH:MM:SS Timezone*.
Export	Allows you to download the events to a local directory path. The filename is appended with the date on which the file is exported. The format of the exported file is `.xls`.

Config

The Config menu includes the following submenus:

Setting Up the SNMP Server for DCNM

When you add a switch to the DCNM inventory, DCNM automatically configures the switch with the following configuration so that the switch knows where to send SNMP traps: snmp-server host dcnm-host-IP traps version 2c public UDP port - 2162

Follow these steps to establish switch-to-DCNM connectivity if you are planning to use a controller deployment.

Procedure

Step 1 To ensure that DCNM receives SNMP traps from the switches, specify the IP address (or VIP address for native HA) to which the switches send the SNMP traps by configuring DCNM server property `trap.registaddress=dcnm-ip` under **Administrator > Server Properties**.

Step 2 For an Inband environment, use the `pmn_telemetry_snmp` CLI template that is packaged along with the Cisco DCNM Application, to configure more SNMP settings on the switch. For more information, see Switch Global Config, on page 187.

AMQP Notifications

For all DCNM operations (such as Host Alias, Host Policy, and so on), AMQP notifications are sent. For operations triggered by the switch and received through telemetry (such as Flow Status), Cisco DCNM

periodically checks for new events and generate appropriate notifications. This time period can be configured by setting the "AMQP_POLL_TIME" value in the `server.properties`.

To update the `server.properties` file and change AMQP poll interval, perform the following:

1. Locate the `server.properties` file that is located at the following location:

   `/usr/local/cisco/dcm/fm/conf/`
2. Edit the line AMQP_POLL_TIME based on the required poll interval. Poll interval value is in minutes.

   `AMQP_POLL_TIME=5`

   The poll interval is set to 5 minutes. By default, the poll interval is set to 2 minutes.
3. Restart the DCNM server to apply the changes that are made in the `server.properties` file, using the command:

   appmgr restart dcnm—for Standalone deployment

   appmgr restart ha-apps—for Native HA deployment



Note AMQP port 5672 is blocked to ensure AMQP always uses TLS or secure connection.

To open the port, log in to the Cisco DCNM server as a root user, and run the following command: **iptables -t mangle -I BUILTIN-FW-SERVICES -p tcp -m tcp --dport 5672 -j ACCEPT**

AMQP Notification Components

- **Routing Key**

  The routing key is an address that the exchange may use to decide how to route the message. This is similar to a URL in HTTP. Most exchange types use the routing key to implement routing logic, but user may choose to ignore it and filter on some other criteria such as message contents. DCNM PMN additionally includes routing key criteria in message header properties.

- **Routing Key Format**

  The routing key of DCNM PMN AMQP for object notification has following format: `Severity.Operation.ObjectType`

  Example: `info.com.cisco.dcnm.event.pmn.create.host`

Key Identifier	Details
Severity	Message Severity (Info/Warning/Error)
Operation	Create/Update/Delete/Discover/Apply/ Establish/Deploy/SwitchReload/DCNM
Object Type	Object involved in notification includes Host Alias, Host, Host Policy, Flow Policy, Flow, Switch, DCNM.

- **Message Properties**

  Message includes following properties and header which can be used for content parsing.

Property	Value
priority	Message priority. Its default value is 0.
delivery_mode	Delivery mode used for the message. Its default value is 2 (persistent), which means the message is stored both in-memory and on disk.
content_encoding	UTF-8
content_type	MIME type of message content. The default value is application/json.
headers	List of name-value pairs about the message. • Severity—Message Severity (Info/Warning/Error). • Operation Status—Success/Failure. • Operation—Create/Update/Delete/Discover/Apply/Establish/Deploy/SwitchReload/DCNM. • Bulk—True/False indicates bulk operation. • Type—Object involved in notification such as Host Alias, Host, Host Policy, Flow Policy, Flow, Switch, DCNM. • User—Logged-in user who performed the action. • Event—Message sent (for backwards compatibility).
message_id	Message ID

- **Notification Body**

  DCNM notification payload contains necessary information to identify the resources that trigger the notification, as well as link for detailed information retrieval. In case of operation failure, the notification includes the error message with detailed reason.

Switch Global Config

Prior to Release 11, Cisco DCNM Media Controller performed operations such as managing the bandwidth, stitching the flows, host link bandwidth, and so on. Beginning with Release 11, DCNM allows two major operations.

- Monitor the network.
- Configure host and flow policies.

DCNM monitors the Flow Status, Discovered Host, Applied Host Policies, and other operations using Telemetry. For any operations triggered by the switch and received through telemetry (e.g. Flow Established), DCNM periodically checks for new events and generate appropriate notification.

If `pmn.deploy-on-import-reload.enabled` server property is set to true, during a switch reload, when DCNM receives switch coldStartSNMPtrap, it will push Global Config, and Host and Flow policies that are showing 'Deployment Status=Successes' to the switch automatically. The switch telemetry and SNMP configuration can be deployed on demand by using DCNM packaged `pmn_telemetry_snmp` CLI template via **Configure > Templates > Template Library**.

Navigate to **Cisco DCNM Web UI > Media Controller > Global > Config** to set or modify Switch Global configuration and WAN links.

When DCNM is installed in Media Controller Deployment mode, you can deploy policies the unicast bandwidth, Any Source Multicast (ASM) range, and WAN links through **Web UI > Media Controller > Global > Config**.

After you deploy the DCNM in Media Controller mode, configure the bandwidth and ASM. The remaining percentage of the bandwidth is utilized by the multicast traffic. DCNM acts like a Master Controller, and deploy the bandwidth and ASM configurations to all the switches in the fabric.

Navigate to **Cisco DCNM Web UI > Media Controller > Global > Config > Switch Global Config** to configure the global parameters.



Note A user with the network operator role in DCNM cannot save, deploy, undeploy, add or delete ASM, or edit the unicast bandwidth reservation percentage.

AMQP Notifications

As Cisco DCNM uses Telemetry to fetch data from the Fabric, the flow status and AMQP notifications may not reflect the current state in real time. It periodically checks new events and generate appropriate notification. Also, flows are no longer limited to a single spine and may take N or W or M shape. Host policies are applied based on the switch interface configuration and not just-in-time (JIT). All these architecture changes influence current AMQP messages and trigger time. By default, poll interval is set to 2 minutes. For more information, see AMQP Notifications, on page 185.

Unicast Bandwidth Reservation

You can configure the server to allot a dedicated percentage of bandwidth to unicast traffic. The remaining percentage is automatically reserved for multicast traffic.

In the Unicast Bandwidth Reservation (%) field, enter a numeric value to configure the bandwidth.

ASM Range

Any Source Multicast (ASM) is a PIM tree building mode that uses shared trees to discover new sources and receivers as well as source trees to form shortest paths from receivers to sources. ASM provides discovery of multicast sources.

You can configure the ASM range by specifying the IP address and the subnet mask.

In the ASM/Mask field, enter the IP address and subnet mask defining the multicast source. Click **Add** icon to add the multicast address to the ASM range. You can add multiple ASM ranges. To delete an ASM range, select the check box next to the ASM/Mask in the table and click **Delete** icon.

After you configure the Unicast Bandwidth Reservation and ASM range, you can perform the following operations to deploy these configurations to the switches.

Table 37: Operations on the Global Config screen

Icon	Description
Save	Click **Save** to save the configurations.
Deploy	To deploy the configuration, you can choose one of the following from the drop-down list: • **All**—Deploys both ASM and Bandwidth configuration to all switches. • **Unicast BW**—Deploys only unicast bandwidth configuration. • **ASM**—Deploys only the ASM configuration. • **All Failed**—Deploys all failed deployments. Success or Failed message appears next to each of the ASM range in the table.
Undeploy	To undeploy the configuration, you can choose one of the following from the drop-down list: • **All**—Undeploys both ASM and Bandwidth configuration to all switches. • **Unicast BW**—Undeploys only unicast bandwidth configuration. • **ASM**—Undeploys only the ASM configuration.
Status	Bandwidth reservation status specifies if the bandwidth deployment was success, or failed or not deployed. ASM/Mask Status field displays if the ASM and Mask configuration was deployed successfully, or failed or not deployed.
History	Click the respective History link to view the deployment history for Unicast Bandwidth and ASM deployments.

The following table describes the fields that appear on the Deployment History.

Table 38: Deployment History Field and Description

Field	Description
Switch Name	Specifies the switch name in the fabric on which the configuration was deployed.

Field	Description
Action	Specifies the action that is performed on the switch - **Deploy** or **Undeploy**.
Deployment Status	Displays the status of deployment. It shows if the deployment was Success or Failed.
Deployment Date/Time	Displays the date and time when the deployment was initialized.
Failed Reason	Specifies the reason why the deployment failed.
Show	From the drop-down list, choose an appropriate filter. • Quick Filter - A search field appears in every column. You can enter a search string to filter. • Advanced Filter - In the Advanced Filter screen, select the All or Any radio button in the Match field. In the Select Filter field, select the category from the drop-down list. Select an appropriate condition from the drop-down field in the next field. Enter a search string in the next field. Click **Add** icon to add another filter. Click **Remove** icon to delete the filter. Click **Clear** to clear all the filters. Click **Apply** to activate the filters, and view the filtered events. Click **Save** to save the applied filter. Click **Cancel** to discard the advanced filters. • All - This removes all the filters and displays the complete deployment history. • Manage Preset Filters - Select an appropriate filter from the drop-down list. Click Edit to modify the filter parameters. Click **Remove** to delete the filter. Click **Cancel** to discard the changes and revert to Deployment History.
Total	Displays the total number of events on the Deployment History page.

After deploying the global configurations, configure the WAN for each switch in your network.

WAN Links

Beginning with Release 11, Cisco DCNM Web UI allows you to configure WAN links for each switch in your fabric.

The external end devices can connect to the network through a Border Leaf and PIM router. The interface that connects the PIM router to the Border Leaf is called WAN Link.

Note A user with the network operator role in DCNM cannot save, deploy, undeploy, or edit WAN links.

1. From the Select a Switch drop-down list, choose a switch in the fabric for which you want to establish WAN links.

   The list of interfaces on the switch is populated in the following table.

   Note The switches that are a part of the fabric appear in the drop-down list.

2. In the WAN Links column, from the drop-down list, choose **Yes** or **No** to designate the interface as a WAN link.
3. Click **View All Deployed WAN Links** to view the Switch Name, Switch IP Address, and Interface Name which is configured as a WAN link. You can choose an appropriate filter to view the WAN links.
4. Click **Save** to save the selection on interfaces as WAN links and other configuration changes.
5. Click **Deploy** to configure the interfaces as WAN links.
6. Click **Undeploy** to remove the WAN links from the switch.

The following table describes the fields that appear on this page.

Table 39: WAN Links Table Field and Description

Field	Description
Status	Specifies if the WAN links are deployed or undeployed on the selected switch.
History	Click this link to view the deployment history. For description about the fields that appear on this page, see the table below.
Interface Name	Specifies the interface which is connected as a WAN link to the end device and this interface will be in Layer 3.
Admin Status	An up arrow depicts that the status is up. A down arrow implies that the status is down.
Oper Status	An up arrow depicts that the operational state of the interface is up. A down arrow implies that the status is down.

Field	Description
WAN Links	From the drop-down, list you can choose to designate this interface as a WAN link. • Select **Yes** to configure the interface as a WAN link. • Select **No** to remove the interface as a WAN link.
Deployment Status	Specifies if the interface is deployed or not.

The following table describes the fields that appear on the Deployment History.

Table 40: Deployment History Field and Description

Field	Description
Switch Name	Specifies the switch name in the fabric on which the configuration was deployed.
Action	Specifies the action that is performed on the switch - **Deploy** or **Undeploy**.
Deployment Status	Displays the status of deployment. It shows if the deployment was Success or Failed.
Deployment Date/Time	Displays the date and time when the deployment was initialized.
Failed Reason	Specifies the reason why the deployment failed.

Field	Description
Show	From the drop-down list, choose an appropriate filter. • Quick Filter - A search field appears in every column. You can enter a search string to filter. • Advanced Filter - In the Advanced Filter screen, select the All or Any radio button in the Match field. In the Select Filter field, select the category from the drop-down list. Select an appropriate condition from the drop-down field in the next field. Enter a search string in the next field. Click **Add** icon to add another filter. Click **Remove** icon to delete the filter. Click **Clear** to clear all the filters. Click **Apply** to activate the filters, and view the filtered events. Click **Save** to save the applied filter. Click **Cancel** to discard the advanced filters. • All - This removes all the filters and displays the complete deployment history. • Manage Preset Filters - Select an appropriate filter from the drop-down list. Click Edit to modify the filter parameters. Click **Remove** to delete the filter. Click **Cancel** to discard the changes and revert to Deployment History.
Total	Displays the total number of events on the Deployment History page.

DCNM Read-Only Mode for Media Controller

From Cisco DCNM Release 11.1(1), you can use the **pmn.read-only-mode.enabled** server property in DCNM. This property allows you to use the DCNM media controller deployment for only monitoring purposes and not as a policy manager. You can set this property to **true** or **false**. By default, the **pmn.read-only-mode.enabled** server property is set to **false**.

After you modify the **pmn.read-only-mode.enabled** server property, restart DCNM by using the **appmgr restart DCNM** command for the property to take effect.

In a DCNM Native HA setup, you need to follow the standard method of modifying any server property file:

1. Set the server property in the `server.properties` file.
2. Use the **appmgr stop all** command on the secondary appliance and then on the primary appliance.
3. Use the **appmgr start all** command on the primary appliance and then on the secondary appliance for the property to take effect.

Starting from Cisco DCNM Release 11.3(1), Host Policies, Flow Policies, and Global menu items are displayed in the Media Controller deployment in DCNM Read-only mode. DCNM retrieves information about the host policies, flow policies, and global configuration from each switch in the fabric and displays the retrieved information. The information that is displayed is specific to each switch.

Static receiver in read-only mode will not read the static receiver configuration from the device and populate the database. To check the static receivers configured on the switch, you can use the existing GET static receiver API or use the new REST API GET **/pmn/switches/static-receiver-discovery/{switchIp}** to get static receiver from a given switch IP address.

We recommend that you to take a decision to use DCNM in either the read-only (RO) or read-write (RW) mode when you perform a fresh install of DCNM. After you configure policies or import policies into DCNM, or deploy policies to switches, do not modify DCNM from RO to RW or vice-versa. You can first remove policies configuration in DCNM and switches, and then convert DCNM mode to RO or RW, that is, undeploy (default and custom host-policies, default and custom flow-policies, and global config) and delete all custom policies from DCNM. Similarly, delete any existing policies deployed by DCNM on switches. After DCNM is in the RO mode, you can apply policies on switches directly. In case of DCNM being configured in the RW mode, you can deploy policies from DCNM GUI.

A user is not expected to convert DCNM to the RO or RW mode if any of following cases are true:

- If DCNM already contains policies, that is, host policies, flow policies, and global config.
- If a DCNM instance has deployed policies to switches.
- If switches managed in DCNM are already configured with policies.

Host Policies - DCNM Read-Only Mode

Navigate to **Media Controller > Host > Host Policies** in DCNM Read-only mode to display the host policies for a switch. By default, information is displayed for the first switch in the **Select Switch** drop-down list. You can select another switch for which you want the information to be displayed from this drop-down list.

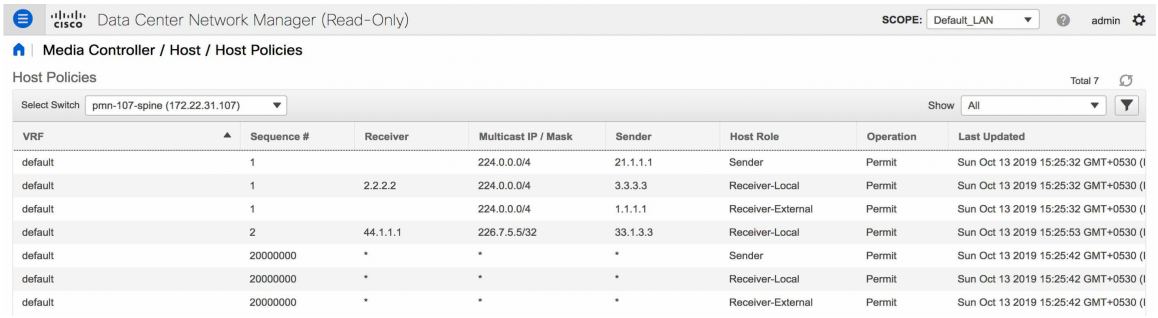


Table 41: Host Policies Table Field and Description

Field	Description
VRF	Specifies the VRF instance on the switch where the policy is defined.
Sequence #	Specifies the sequence number of the policy. This field displays 20000000 for default host policies.
Host Name	Specifies the host ID.

Field	Description
Receiver	Specifies the IP address of the receiving device.
Multicast IP / Mask	Specifies the multicast IP address and mask for the host.
Sender	Specifies the IP Address of the sender.
Host Role	Specifies the host device role. The host device role is one of the following: • Sender • Receiver-External • Receiver-Local
Operation	Specifies if the operation of the host policy. The policy has the following operations: • Permit • Deny
Last Updated	Specifies the date and time at which the host policy was last updated. The format is *Day MMM DD YYYY HH:MM:SS Timezone*.

Flow Policies - DCNM Read-Only Mode

Navigate to **Media Controller > Flow > Flow Policies** in DCNM Read-only mode to display the flow policies for a switch. By default, information is displayed for the first switch in the **Select Switch** drop-down list. You can select another switch for which you want the information to be displayed from this drop-down list.

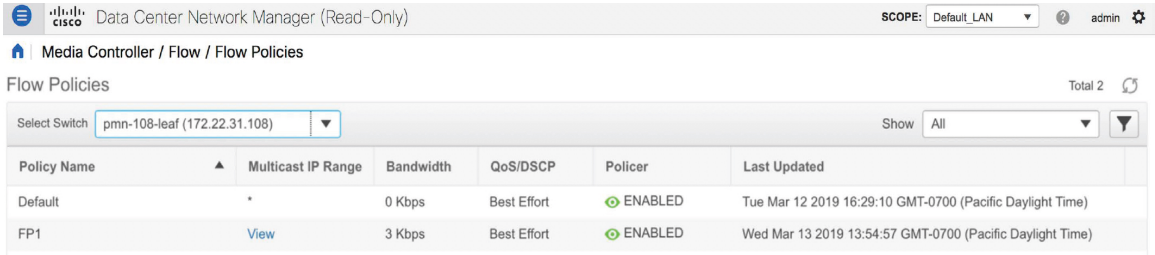


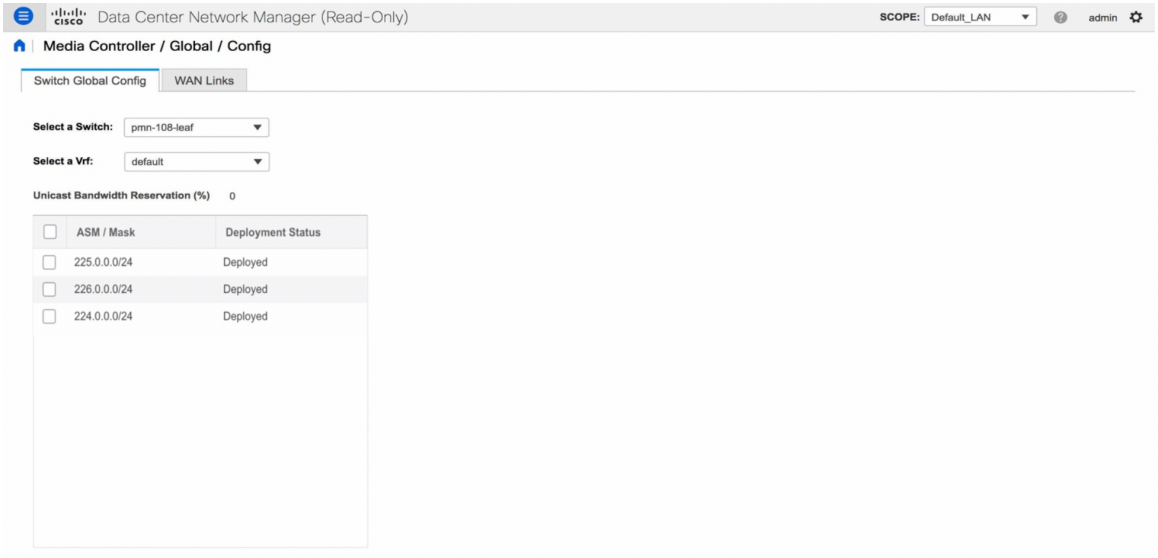
Table 42: Flow Policies Table Field and Description

Field	Description
Policy Name	Specifies the flow policy name.
Multicast IP Range	Specifies the multicast IP address for the traffic.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.
QoS/DSCP	Specifies the Switch-defined QoS Policy.

Field	Description
Policer	Specifies whether the policer for a flow policy is enabled or disabled.
Last Updated	Specifies the date and time at which the flow policy was last updated. The format is *Day MMM DD YYYY HH:MM:SS Timezone*.

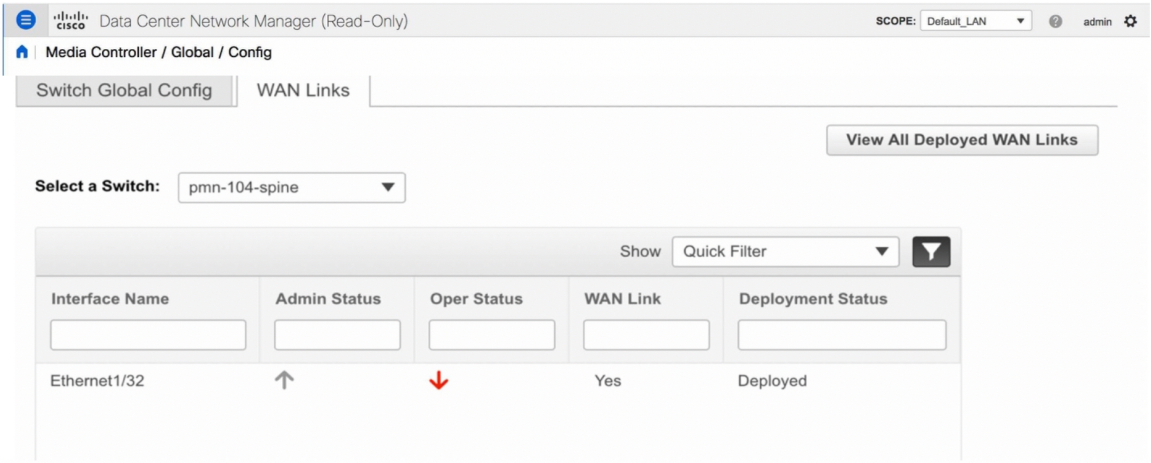
Switch Global Config - Read-Only Mode

Navigate to **Media Controller > Global > Config** to display the Switch Global configuration in DCNM Read-Only mode. You can select a switch from the **Select a Switch** drop-down list to display the switch global configuration that is currently deployed on that switch. You can also select a specific VRF from the **Select a VRF** drop-down list.



WAN Links - Read-Only Mode

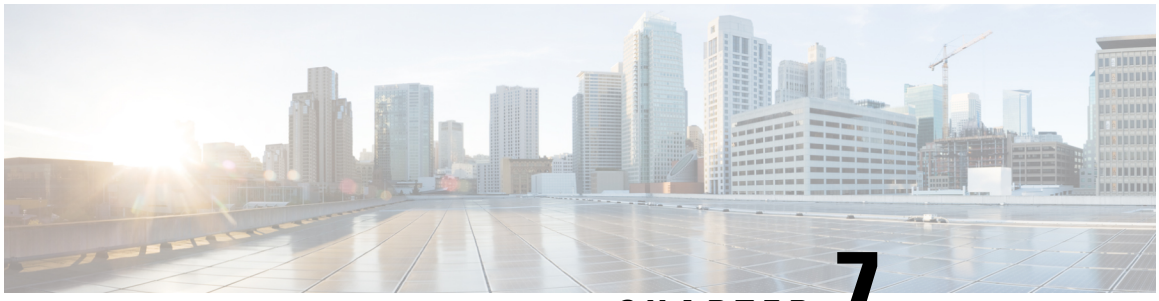
Navigate to **Media Controller > Global > Config** to and click **WAN Links** to display the WAN links in DCNM Read-Only mode. You can select a switch from the **Select a Switch** drop-down list to display the WAN links that are currently deployed on that switch.



The following table describes the fields that appear on the WAN Links tab.

Table 43: WAN Links Table Field and Description

Field	Description
Interface Name	Specifies the interface which is connected as a WAN link to the end device.
Admin Status	An up arrow depicts that the status is up. A down arrow implies that the status is down.
Oper Status	An up arrow depicts that the operational state of the interface is up. A down arrow implies that the status is down.
WAN Links	From the drop-down, list you can choose to designate this interface as a WAN link. • Select **Yes** to configure the interface as a WAN link. • Select **No** to remove the interface as a WAN link.
Deployment Status	Specifies if the interface is deployed as a WAN link or not.



CHAPTER 7

Administration

This chapter contains the following topics:

- DCNM Server, on page 199
- Manage Licensing, on page 210
- Management Users, on page 219
- Performance Setup, on page 226
- Event Setup, on page 228
- Credentials Management, on page 233

DCNM Server

The DCNM Server menu includes the following submenus:

Starting, Restarting, and Stopping Services

By default, the ICMP connectivity between DCNM and its switches validates the connectivity during Performance Management. If you disable ICMP, Performance Management data will not be fetched from the switches. You can configure this parameter in the **server properties**. To disable ICMP connectivity check from Cisco DCNM Web UI, choose **Administration > DCNM Server > Server Properties**, and set `skip.checkPingAndManageable` parameter value to `true`.

To clean up the performance manager database (PM DB) stale entries, start, restart, or stop a service, from the Cisco DCNM Web UI, perform the following steps:



Note During restart, the Performance Manager waits for 20minutes for the Elasticsearch to become operational. After 20minutes, the Performance Manager aborts. Click the **Re-init Elasticsearch DB Schema** icon in the **Actions** column for the **Performance collector** service.

Procedure

Step 1 Choose **Administration > DCNM Server > Server Status**.

The **Status** window appears that displays the server details.

Step 2 In the **Actions** column, click the action you want to perform. You can perform the following actions:

- Start or restart a service.
- Stop a service.
- Clean up the stale PM DB entries.
- Reinitialize the Elasticsearch DB schema.

Step 3 View the status in the **Status** column.

What to do next

See the latest status in the **Status** column.

Using the Commands Table

The commands table contains links to commands that launch new dialog boxes to provide information about the server status and server administrative utility scripts. You can execute these commands directly on the server CLI.

- **ifconfig**: click this link to view information about interface parameters, IP address, and netmask used on the Cisco DCNM server.
- **appmgr status all**: click this link to view the DCNM server administrative utility script that checks the status of different services currently running.
- **appmgr show vmware-info**: click this link to view information about the CPU and Memory of Virtual Machine.
- **clock**: click this link to view information about the server clock details such as time, zone information.



Note The commands section is applicable only for the OVA or ISO installations.

Customization

From Cisco DCNM Release 11.3(1), you can modify the background image and message on the Web UI login page. This feature helps you to distinguish between the DCNM instances, when you have many instances running at the same time. You can also use a company-branded background on the login page. Click on Restore Defaults to reset the customizations to their original default values.

To remove the customizations and restore to the default values, click **Restore defaults**.

Login Image

This feature allows you to change the background image on the Cisco DCNM Web UI login page. If you have many instances of DCNM, this will help you identify the correct DCNM instance based on the background image.

To edit the default background image for your Cisco DCNM Web UI login page, perform the following steps:

1. Choose **Administration > DCNM Server > Customization**.
2. In the Login Image area, click **Add (+)** icon.

   Browse for the image that you need to upload from your local directory. You can choose any of the following format images: JPG, GIF, PNG, and SVG.
3. Select the image and click **Open**.

   A status message appears on the right-bottom corner.

```
Login image
Upload Successful
```



Note We recommend that you upload a scaled image for fast load times.

   The uploaded image is selected and applied as the background image.
4. To choose an existing image as login image, select the image and wait until you see the message on the right-bottom corner.
5. To revert to the default login image, click **Restore Defaults**.

Message of the day (MOTD)

This feature allows you to add a message to the Cisco DCNM Web UI login page. You can a list of messages that will rotate on the configured frequency. This feature allows you to convey important messages to the user on the login page.

To add or edit the message of the day on the Cisco DCNM Web UI login page, perform the following steps:

1. Choose **Administration > DCNM Server > Customization**.
2. In the **Message of the day (MOTD)** field, enter the message that must appear on the login page.
3. Click **Save**.

Viewing Log Information

You can view the logs for performance manager, SME server, web reports, web server, and web services. These processes have no corresponding GUI that allows you to view information about these log files. If you see errors, preserve these files for viewing.

Beginning with Release 11.2(1), for DCNM OVA and DCNM ISO installations, all log files with .log extension are also listed.



Note Logs cannot be viewed from a remote server in a federation.

To view the logs from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > Logs**.

You see a tree-based list of logs in the left column. Under the tree, there is a node for every server in the federation. The log files are under the corresponding server node.

Step 2 Click a log file under each node of the tree to view it on the right.

Step 3 Double-click the tree node for each server to download a ZIP file containing log files from that server.

Step 4 (Optional) Click **Generate Techsupport** to generate and download files required for technical support.

This file contains more information in addition to log files.

Note A TAR.GZ file will be downloaded for OVA and ISO deployments, and a ZIP file will be downloaded for all other deployments. You can use the use **appmgr tech_support** command in the CLI to generate the techsupport file.

Step 5 (Optional) Click the **Print** icon on the upper right corner to print the logs.

Server Properties

You can set the parameters that are populated as default values in the DCNM server.

To set the parameters of the DCNM server from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > Server Properties**.

Step 2 Click **Apply Changes** to save the server settings.

Configuring SFTP/TFTP/SCP Credentials

A file server is required to collect device configuration and restoring configurations to the device.

To configure the SFTP/TFTP/SCP credentials for a file store from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > Archive FTP Credentials**.

The **Archive FTP Credentials** window is displayed.

Note The credentials are auto-populated for fresh OVA and ISO installations.

Step 2 In the **Server Type** field, use the radio button to select **SFTP**.

Note
- You must have an SFTP server to perform backup operation. The SFTP server can be an external server. The SFTP directory must be an absolute Linux/SSH path format and must have read/write access to the SFTP User.
- If you are using an external server, enter its IP address in the **server.FileServerAddress** field in **Administration > DCNM Server > Server Properties**.
- If the **nat.enabled** field under **Administration > DCNM Server > Server Properties** is true, you must enter the NAT device IP in the **server.FileServerAddress** field and the SFTP server must be local.

a) Enter the **User Name** and **Password**.

Note From Release 11.3(1), for OVA/ISO installations, use the **sysadmin** user credentials to access the root directory.

b) Enter the **Directory** path.

The path must be in absolute Linux path format.

If SFTP is unavailable on your device, you can use third-party SFTP applications, such as, mini-SFTP, Solarwinds, and so on. When you use an external SFTP, you must provide the relative path in the STFP Directory Path. For example, consider the use cases at the end of this procedure.

Note From Release 11.3(1), for OVA/ISO installations, enter directory as `/home/sysadmin`.

c) From the **Verification Switches** drop-down list, select a switch.
d) Click **Apply** to save the credentials.
e) Click **Verify & Apply** to verify if SFTP and switch have connectivity and save 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 appears. Navigate to **Configure > Backup > Switch Configuration > Archive Jobs > Job Execution Details** to view the number of successful and unsuccessful switches.

Step 3 In the **Server Type** field, use the radio button to select **TFTP**.

Cisco DCNM uses a local 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 receive a *permission denied* error. You can change your credentials in the **Discovery** window. Navigate to **Inventory > Discovery**.

a) From the **Verification Switch** drop-down list, select a switch.
b) Click **Apply** to save the credentials everywhere.
c) Click **Verify & Apply** to verify if TFTP and switch have connectivity and save the configuration.

If there are any failures during the verification, the new changes are not stored.

Step 4 In the **Server Type** field, use the radio button to select **SCP**.

Note

- You must have an SCP server to perform backup operation. The SCP server can be an external server. The SCP directory must be an absolute Linux/SSH path format and must have read/write access to the SCP User.
- If you are using an external server, enter its IP address in the **server.FileServerAddress** field under **Administration > DCNM Server > Server Properties**.
- If the **nat.enabled** field under **Administration > DCNM Server > Server Properties** is true, you must enter the NAT device IP in the **server.FileServerAddress** field and the server must be local.

a) Enter the **User Name** and **Password**.
b) Enter the **Directory** path.

The path must be in absolute Linux path format.

If SCP is unavailable on your device, use external SCP applications, such as, mini-SCP, Solarwinds, and so on. When you use an external SCP, you must provide the relative path in the SCP Directory Path. For example, consider the use cases at the end of this procedure.

c) From the **Verification Switches** drop-down, select the switch.
d) Click **Apply** to save the credentials everywhere.
e) Click **Verify & Apply** to verify if SCP and switch have connectivity and save 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. To view the number of successful and unsuccessful switches, go to **Configure > Backup > Switch Configuration > Archive Jobs > Job Execution Details**.

Step 5 Choose **Configuration > Templates > Templates Library > Jobs** to view individual device verification status.

The configurations that are backed up are removed from the file server and are stored in the file system.

SFTP Directory Path

Use Case 1:

If Cisco DCNM is installed on Linux platforms, like OVA, ISO, or Linux, and the test folder is located at `/test/sftp/`, you must provide the entire path of the SFTP directory. In the SFTP Directory field, enter `/test/sftp`.

Use Case 2:

If Cisco DCNM is installed on the Windows platform, and the test folder is located at `C://Users/test/sftp/`, you must provide the relative path of the SFTP directory. In the SFTP Directory field, enter `/`.

For Example:

- If the path in the external SFTP is `C://Users/test/sftp/`, then the Cisco DCNM SFTP Directory path must be `/`.

- If the path in the external SFTP is `C://Users/test`, then the Cisco DCNM SFTP Directory path must be `/sftp/`.

Examples for SCP Directory Path

Use Case 1:

If Cisco DCNM is installed on Linux platforms, like OVA, ISO, or Linux, and the test folder is located at `/test/scp/`, you must provide the entire path of the SCP directory. In the **SCP Directory** field, enter `/test/scp`.

Use Case 2:

If Cisco DCNM is installed on the Windows platform, and the test folder is located at `C://Users/test/scp/`, you must provide the relative path of the SCP directory. In the **SCP Directory** field, enter `/`.

For Example:

- If the path in the external SCP is `C://Users/test/scp/`, then the Cisco DCNM SCP directory path must be `/`.
- If the path in the external SCP is `C://Users/test`, then the Cisco DCNM SCP directory path must be `/scp/`.

Modular Device Support

To support any new hardware that does not require many major changes, a patch can be delivered instead of waiting for the next DCNM release. **Modular Device Support** helps to deliver and apply the DCNM patch releases. An authorized DCNM administrator can apply the patch to the production setup. Patch releases are applicable for the following scenarios:

- Support any new hardware, like chassis or line cards
- Support latest NX-OS versions
- Support critical fixes as patches

To view the patch details from Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > Modular Device Support**.

You see the **DCNM Servers** column on the left in the window and **Modular Device support information** window on the right.

Step 2 Expand **DCNM Servers** to view all the DCNM servers.

It includes the list of patches installed along with the version number, corresponding platforms supported, chassis supported, NX-OS version supported, PID supported, backup directory and the last patch deployment time in the **Modular Device support information** table.

What to do next

For more details about how to apply and rollback a patch, go to http://www.cisco.com/go/dcnm for more information.

Managing Switch Groups

You can configure switch groups by using Cisco DCNM Web UI. You can add, delete, or move a switch to a group, or move switches from a group to another group.

Creating switch groups will help you to manage switches because they are grouped logically. For example, you can create host or flow policies for switches in a specific switch group instead of creating it for all the switches. Similarly, you can view the flow topology for a specific switch group containing switches.

The switch groups are listed under the **SCOPE** drop-down list at the top right part of windows under **Media Controller**.



Note The hostname of the switch should be unique across all the switch groups. You cannot have the same hostname and management IP address for two different switches in two switch groups.

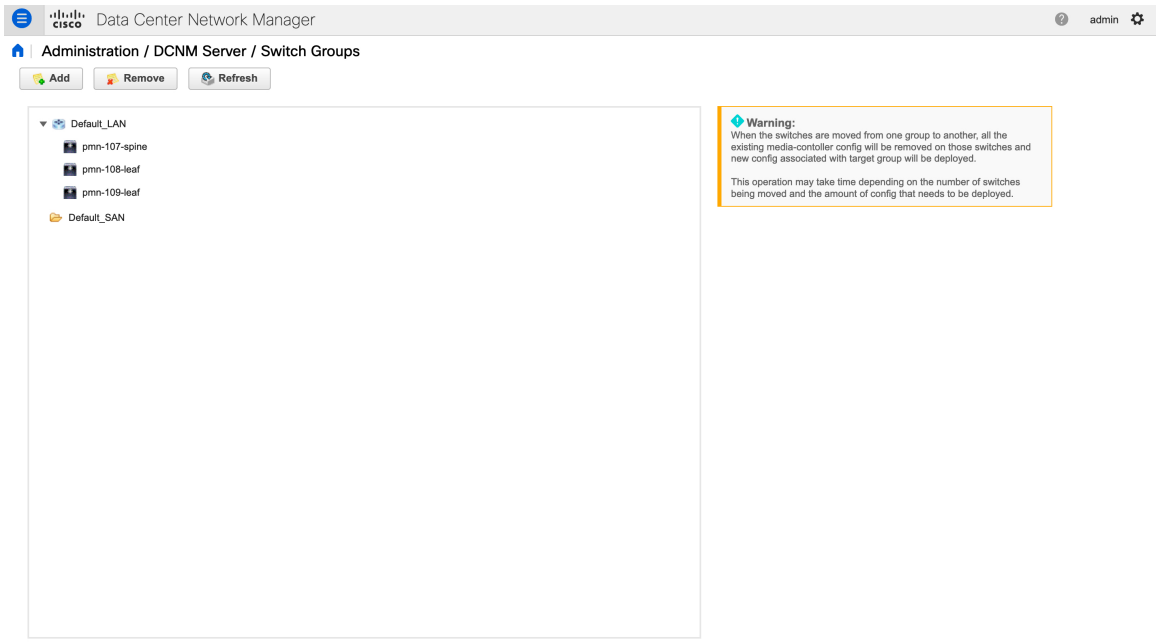
This section contains the following:

Adding Switch Groups

To add switch groups from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > Switch Groups**.



Step 2 Click the **Add** icon.

The **Add Group** window is displayed, that allows you to enter the name for the switch group.

Step 3 Enter the name of the switch group and click **Add** to complete adding the switch group.

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.

Whenever you add a new switch group, the default policies are automatically created for this switch group.

Note When you discover and add a switch in DCNM, you can choose the switch group for the new switch. For more information, see *Adding LAN Switches*.

Removing a Group or a Member of a Group

You can remove a group or a member of the group from the Cisco DCNM Web UI. When you remove a group, the ethernet switches of the deleted group are moved to the default LAN group. When you remove a member of a group, the member is moved to the default LAN group.

To remove a group or a member of a group from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose the switch group or members of a group that you want to remove.

Step 2 Click the **Remove** icon.

A dialog box prompts you to confirm the deletion of the switch group or the member of the group.

Note When you remove a switch from a switch group, a dialog box does not pop-up for a confirmation. The switch is moved to the **Default_LAN** switch group after you click the **Remove** icon. A switch can be removed from the **Default_LAN** switch group by navigating to **Inventory > Discovery > LAN Switches** and using the delete option. If you delete a switch, it will be not managed by DCNM.

Step 3 Click **Yes** to delete or **No** to cancel the action.

Note **Default_LAN** is the default group that cannot be removed or deleted.

Moving a Switch to Another Group

To move a switch to another group from the Cisco DCNM Web UI, perform the following steps:



Warning When the switches are moved from one group to another, all the existing media-controller config will be removed on those switches and new config associated with target group will be deployed.

This operation may take time depending on the number of switches being moved and the amount of config that needs to be deployed.

Procedure

Step 1 Select a switch.

Step 2 Drag the highlighted switch to another group. To move multiple switches across different switch groups, use Ctrl key or Shift key.

Native HA

Before you begin



Note Ensure that you clear your browser cache and cookies everytime after a Federation switchover or failover.

Procedure

Step 1 By default, DCNM is bundled with an embedded database engine PostgreSQL. The native DCNM HA is achieved by two DCNMs running as **Active / Warm Standby**, with their embedded databases synchronized in real time. So once the active DCNM is down, the standby takes over with the same database data and resume the operation. The *standby host database down* scenario is documented after this procedure.

Step 2 From the menu bar, choose **Administration > DCNM Server > Native HA**.

You see the **Native HA** window.

Step 3 You can allow manual failover of DCNM to the standby host by clicking the **Failover** button, and then click **OK**.

- Alternatively, you can initiate this action from the Linux console.
  a. SSH into the DCNM active host.
  b. Enter " " /usr/share/heartbeat/hb_standby”

Step 4 You can allow manual syncing database and disk files to standby host by clicking **Force Sync**, and then click **OK**.

Step 5 You can test or validate the HA setup by clicking **Test** and then click **OK**.

What to do next

Some HA troubleshooting scenarios are noted in this sub section.

The standby host database is down: Typically, the DCNM database (PostgreSQL) is up on the active and standby hosts. In DCNM 10.1 and earlier versions, the standby database can be down due to a database synchronization failure.

- Enter “ps -ef | grep post”. You should see multiple postgres processes running. If not, it indicates that the database is down.
- Restore database data from a backup file that is created at the beginning of database synchronization. Change directory to “/usr/local/cisco/dcm/db”
- Check existence of file replication/ pgsql-standby-backup.tgz. If the file exists, restore database data files:

```
rm -rf    data/*
tar -zxf    replication/ pgsql-standby-backup.tgz    data
/etc/init.d/postgresql-9.4 start
ps -ef | grep post
```

  The active DCNM host will synchronize the two databases.

The TFTP server is not bound to the eth1 VIP address on the active host: The TFTP server should run on the active host (not on the standby host), and it should be bound to the eth1 VIP address. In some setups, the bind address is not the VIP address, as per the TFTP configuration file, and this could cause issues when switches try to use TFTP.

- Enter “grep bind /etc/xinetd.d/tftp” to check if the TFTP configuration file has the right bind address. If the displayed IP address is not the eth1 VIP address, then change the bind address to the VIP address. Repeat the procedure for the standby host. Update the bind address to the VIP address.
- Enter " " /etc/init.d/xinetd restart” on the active host to restart TFTP.



Note The TFTP server can be started or stopped with the “appmgr start/stop ha-apps” command.

Multi Site Manager

Procedure

Step 1 Multi-Site-Manager (MsM) provides a single pane for users to search for switches that are managed by DCNM globally. MSM can do realtime search to find out which switch globally handles the traffic for a given virtual machine based on IP address, name or mac address, and supporting VXLAN basing on segment ID as well. It provides hyperlink to launch the switch only. This window also plays the role of remote site registration. The registration only allows the current DCNM server to access the remote DCNM server or site. For the remote site to access the current DCNM server, registration is required on the remote site as well.

Step 2 Choose **Administration > DCNM Server > Multi Site Manager**.

The MsM window displays the overall health or status of the remote site and the application health.

Step 3 You can search by **Switch, VM IP, VM Name, MAC**, and **Segment ID**.

Step 4 You can add a new DCNM server by clicking **+Add DCNM Server**. The **Enter Remote DCNM Server Information** window opens. Fill in the information that is required and click **OK** to save.

Step 5 Click **Refresh All Sites** to display the updated information.

Manage Licensing

The Manage Licensing menu includes the following submenus:

Managing Licenses

You can view the existing Cisco DCNM licenses by choosing **Administration > Manage Licensing > DCNM**. You can view and assign licenses in the following tabs:

- **License Assignments**
- **Smart License**
- **Server License Files**



Note By default, the **License Assignments** tab appears.

The following table displays the SAN and LAN license information.

Field	Description
License	Specifies SAN or LAN.
Free/Total Server-based Licenses	Specifies the number of free licenses that are purchased out of the total number of licenses. The total number of licenses for new installations are 50. However, the total number of licenses continues to be 500 for inline upgrade.

Field	Description
Unlicensed/Total (Switches/VDCs)	Specifies the number of unlicensed switches or VDCs out of the total number of switches or VDCs.
Need to Purchase	Specifies the number of licenses to be purchased.

This section includes the following topics:

License Assignments

The following table displays the license assignment details for every switch or VDC.

Field	Description
Group	Displays if the group is fabric or LAN.
Switch Name	Displays the name of the switch.
WWN/Chassis ID	Displays the world wide name or Chassis ID.
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: • Permanent • Eval • Unlicensed • Not Applicable • Expired • Invalid
License Type	Displays the license type of the switch that can be one of the following: • DCNM-Server • Switch • Smart • Honor
Expiration Date	Displays the expiry date of the license. **Note** Text under the **Expiration Date** column is in red for licenses, which expire in seven days.
Assign License	Select a row and click this option on the toolbar to assign the license.
Unassign License	Select a row and click this option on the toolbar to unassign the license.

Field	Description
Assign All	Click this option on the toolbar to refresh the table and assign the licenses for all the items in the table.
Unassign All	Click this option on the toolbar to refresh the table and unassign all the licenses.

Note You must have network administrator privileges to assign or unassign licenses.

When the fabric is first discovered and 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. If you have an existing fabric and a new switch is added to the fabric, the new switch is assigned a license if one is available in the file license pool and if it does not already have a switch-based license.

After you register smart license, if you click **Assign License** for a switch that does not have a permanent license, a smart license is assigned to the switch. The priority of licenses that are assigned are in the following order:

1. **Permanent**
2. **Smart**
3. **Eval**

Disabling smart licensing unassigns licenses of switches that were smart-licensed.

The evaluation license is assigned for switches that do not support smart licensing. The license state is **Eval** and the license type is **DCNM-Server**. See *Cisco DCNM Licensing Guide, Release 11.x* to view the list of switches that support smart licensing.

Honor License Mode

From Release 11.3(1), Cisco DCNM Eval license validity is extended from 30 days to 60 days. That implies, after 60 days. Every license has an expiry date attached to it. After the license expires, Cisco DCNM allows you to use all the licensed features. Switches remain in honor mode until the switch is licensed again or the user manually removes the license.

If there are switches in the Honor License mode, an error message appears after you logon to DCNM.

```
************************************
*Your licenses are out of compliance.
Your inventory contains switches that are unlicensed for DCNM Operation*

************************************
```

Go to **Administration > Manage Licensing > DCNM**, In the **Switches/VDCs** table, select the switch and click **Assign License** to renew the license.

Guidelines

- Switches that don’t have a license assigned to them is considered unlicensed. Unlicensed Switches aren’t allowed to use Licensed DCNM features.

- If a switch has an expired EVAL license, it will change from EVAL to Honor mode and the license features continues to be operational.
- You can't assign expired EVAL licenses to the switches.
- Switches with switch-based honor license can't be overwritten with any server-based license.
- When a license is assigned to a discovered switch and a valid license isn't available, then an honor-based license with expiration date will be assigned to the switch.

Nag events for Honor-mode licenses

For every license in honor mode, an event is generated every seven days. A nag event informs the user "DCNM-SAN file license is in honor mode, need to assign/purchase a new license for this switch." Or "DCNM-LAN file license is in honor mode, need to assign/purchase a new license for this switch."

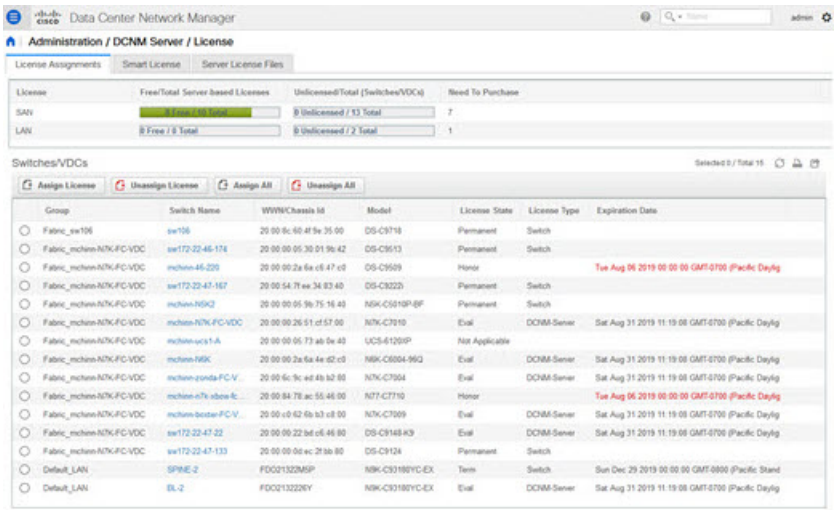
Additional popup notification appears when you logon to Cisco DCNM, to inform that "DCNM-SAN file license is in honor mode, need to assign/purchase a new license for this switch."

Server-based honor license support

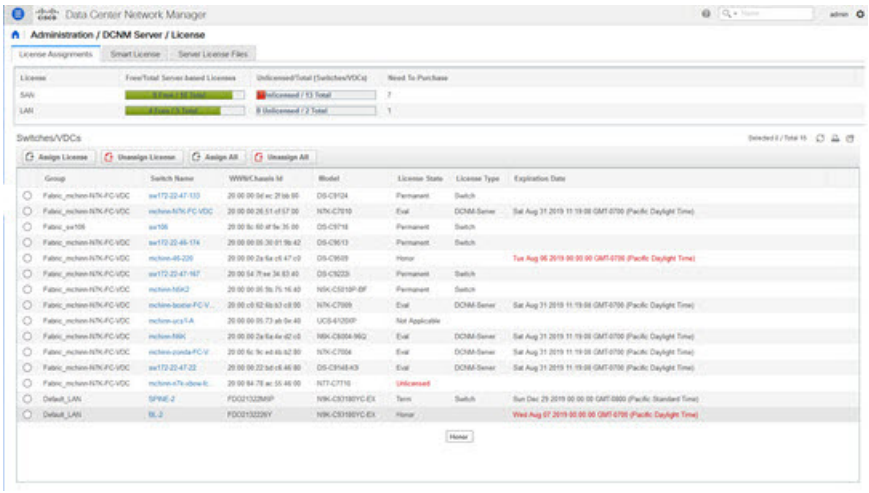
On the DCNM **Web UI > Administration > Manage Licensing > DCNM**, the **Licensed State** column displays **Honor** and **Expiration Date** column displays the date, time, and when the license expired and changed to the Honor mode.

Switches will remain in honor mode after reboot also. To change the license from honor mode, you must manually unassign the license or assign a new valid license to the switch.

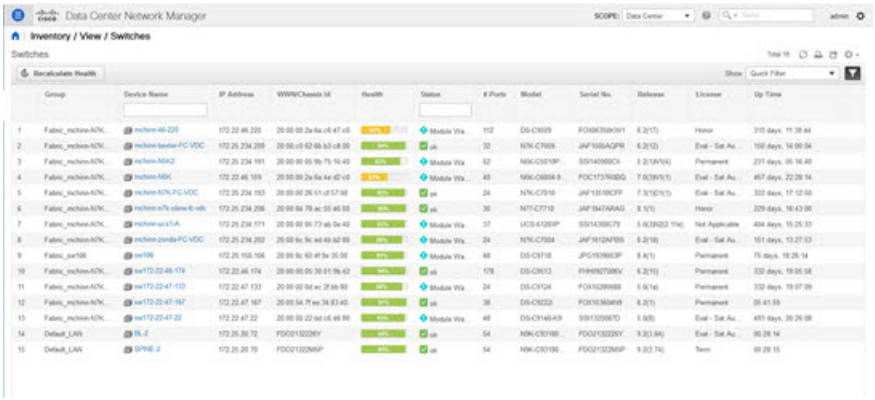
The following image shows license page with a SAN switch in Honor mode.



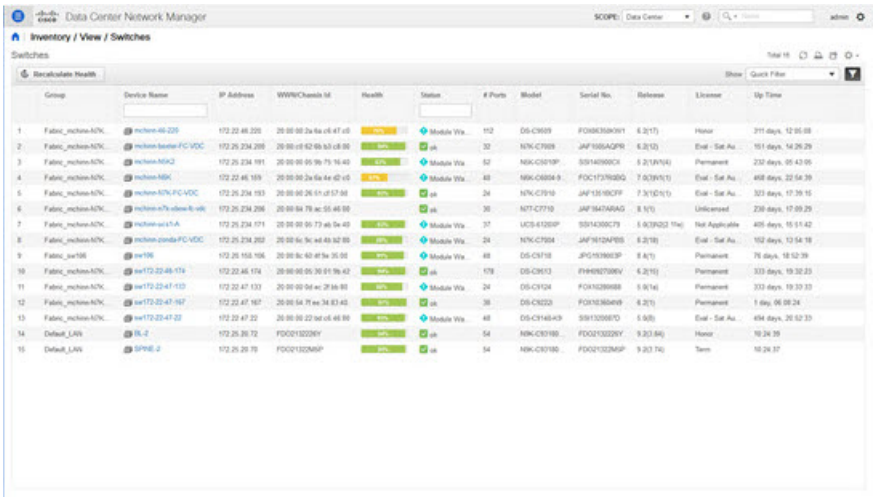
The following image shows license page with a LAN switch in Honor mode.



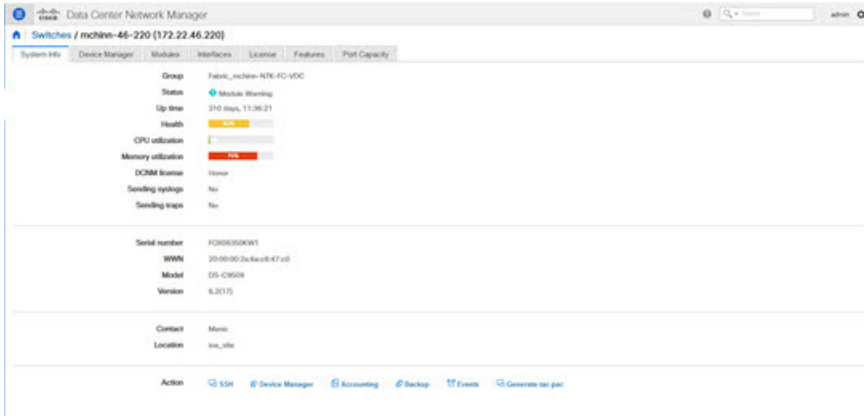
The following image shows the switch table displaying the honor mode of license and term.



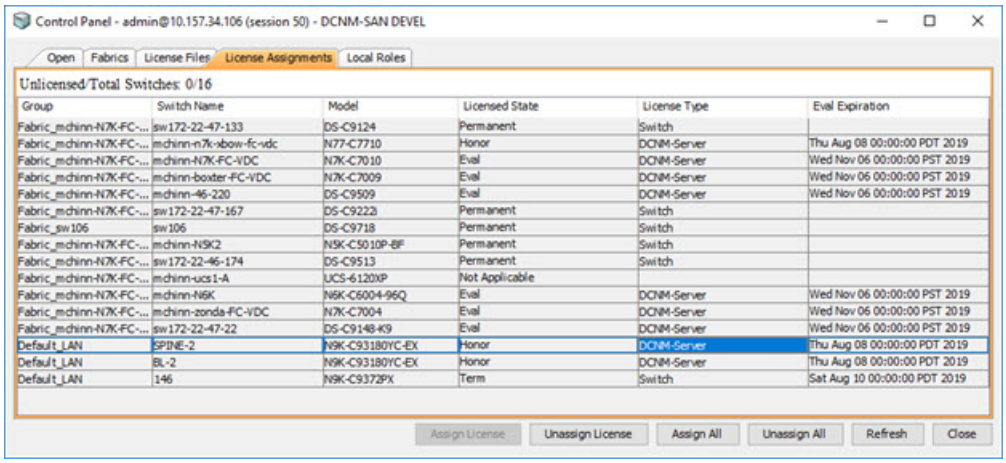
The following image shows Switch Dashboard with a LAN switch in Honor mode license.



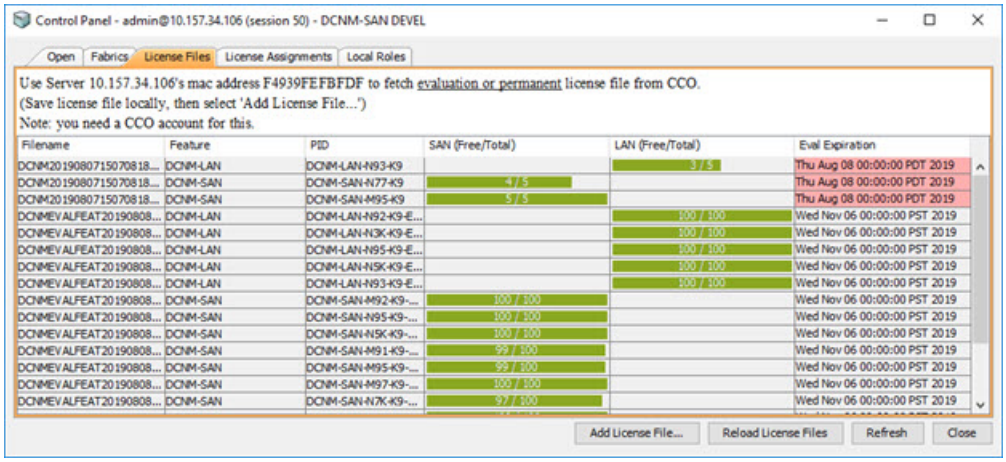
The following image shows Switch Dashboard with a SAN switch in Honor mode license.



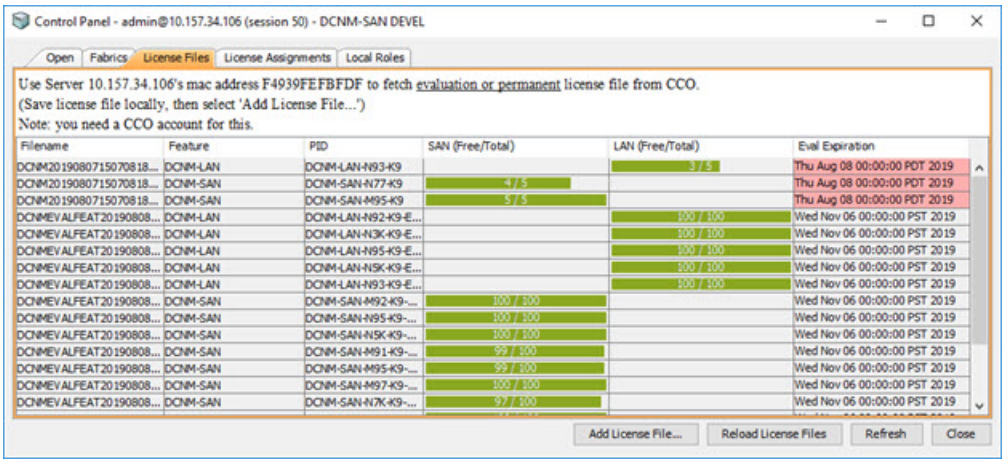
The following image shows the SAN Client License Agreement tab.



The following image shows the **SAN Client License** files tab.



Note Switch-based honor licenses can’t be overwritten with server-based license files.



Server License Files

From Cisco DCNM Web UI, choose **Administration > Manage Licensing > DCNM > Server License Files**. The following table displays the Cisco DCNM server license fields.

Field	Description
Filename	Specifies the license file name.
Feature	Specifies the licensed feature.
PID	Specifies the product ID.
LAN (Free/Total)	Displays the number of free versus total licenses for LAN.
Expiration Date	Displays the expiry date of the license. **Note** Text in the **Expiration Date** field is in Red for licenses that expires in seven days.

Adding Cisco DCNM Licenses

To add Cisco DCNM licenses from Cisco DCNM, perform the following steps:

Before you begin

You must have network administrator privileges to complete the following procedure.

Procedure

Step 1 Choose **Administration > Manage Licensing > DCNM** to start the license wizard.

Step 2 Choose the **Server License Files** tab.

The valid Cisco DCNM-LAN license files are displayed.

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 select the license pack file that you saved on the local machine.

The file is uploaded to the server machine, which is 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 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 is counted.

Switch Features—Bulk Install

From Release 11.3(1), Cisco DCNM allows you to upload multiple licenses at a single instance. DCNM parses the license files and extract the switch serial numbers. It maps the serial numbers in the license files with the discovered fabric to install the licenses on each switch. License files are moved to bootflash and installed.

To bulk install licenses to the switches on the Cisco DCNM Web Client UI, perform the following steps:

1. Choose **Administration > Manage Licensing > Switch features**.
2. In the Switch Licenses area, click **Upload License files** to upload the appropriate license file.

   The Bulk Switch License Install window appears.
3. In the Select file, click **Select License file(s)**.

   Navigate and choose the appropriate license file located in your local directory.

   Click **Open**.
4. Choose the file transfer protocol to copy the license file from the DCNM server to the switch.
   - Choose either **TFTP**, **SCP**, or **SFTP** protocol to upload the license file.

   Note Not all protocols are supported for all platforms. TFTP is supported for Win/RHEL DCNM SAN installation only. However, SFTP/SCP supported for all installation types.
5. Check the **VRF** check box for the licenses to support VRF configuration.

   Enter the VRF name of one of their defined routes.
6. Check the **Overwrite file on Switch** checkbox, to overwrite the license file with the new uploaded license file.

   Note The overwrite command copies the new file over the existing one in boot flash. If the previous license already installed, it won't override the installation.
7. In the DCNM Server credentials, enter the root username and password for the DCNM server.

Enter the authentication credentials for access to DCNM. For DCNM Linux deployment, this is the username. For OVA\ISO deployments, use the credentials of the **sysadmin** user.

8. Click **Upload**.

   The License file is uploaded to the DCNM. The following information is extracted from the license file.

   - Switch IP – IP Address of the switch to which this license is assigned.
   - License File – filename of the license file
   - Features List –list of features supported by the license file

9. Select the set of licenses that you want to upload and install on their respective switches. A license file is applicable for a single specific switch.

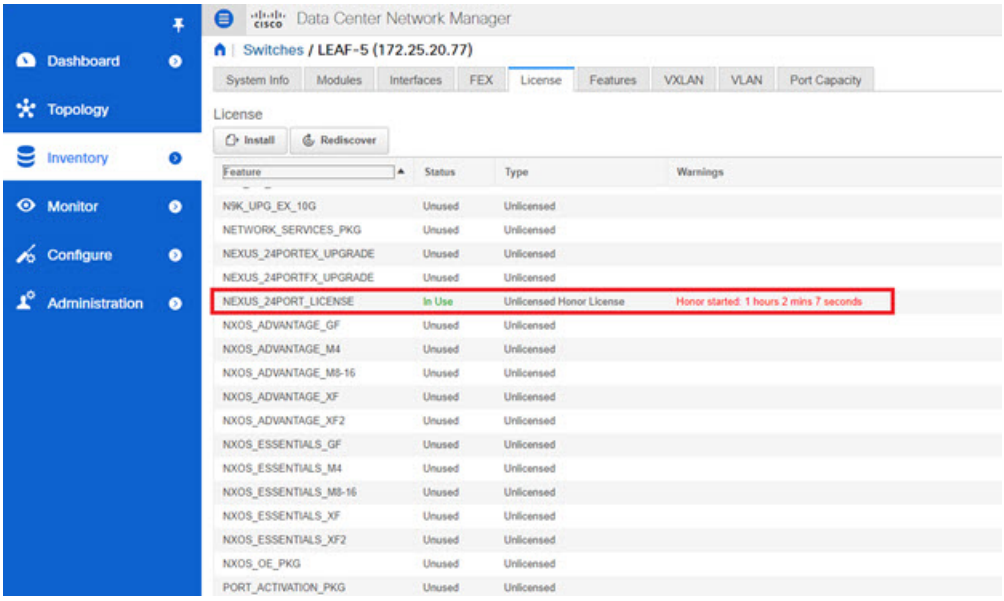
10. Click **Install Licenses**.

    The selected licenses are uploaded and installed on their respective switches. Status messages, including any issues or errors are updated for each file as it completes.

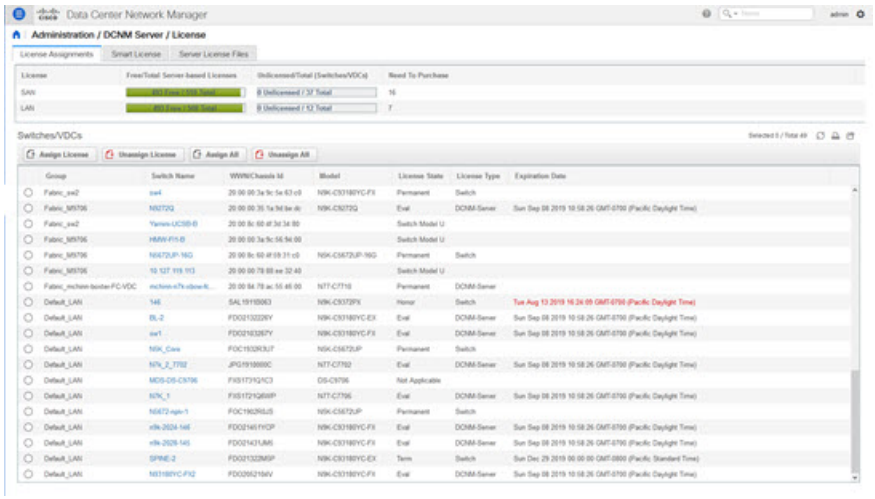
11. After the license matches with respective devices and installs, the **License Status** table displays the status.

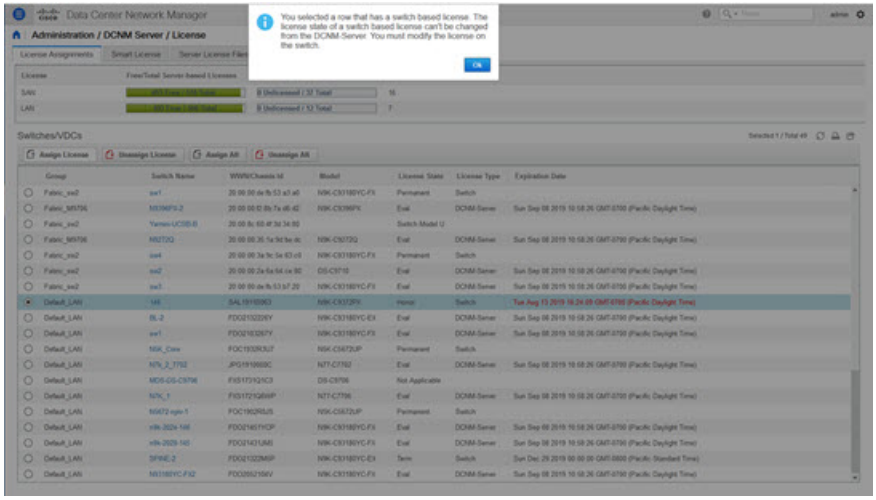
Switch-based honor license support

On the DCNM **Web UI > Inventory > Switch > License**, the **Type** column displays "Unlicensed Honor License" and **Warnings** column displays **Honor started: …** with elapsed time since the license was changed to the Honor mode.



Note Switch-based honor licenses can't be overwritten with server-based license files.





Management Users

Note Every time you login to DCNM, the DCNM server fetches information from the ISE server for AAA authentication. The ISE server will not authenticate again, after the first login.

The Management Users menu includes the following submenus:

Remote AAA

To configure remote AAA from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > Management Users > Remote AAA Properties**.

The AAA properties configuration window appears.

Step 2 Use the radio button to select one of the following authentication modes:

- Local: In this mode the authentication authenticates with the local server.
- Radius: In this mode the authentication authenticates against the RADIUS servers specified.
- TACACS+: In this mode the authentication authenticates against the TACACS servers specified.
- Switch: In this mode the authentication authenticates against the switches specified.
- LDAP: In this mode the authentication authenticates against the LDAP server specified.

Step 3 Click **Apply**.

Note Restart the Cisco DCNM LAN services if you update the Remote AAA properties.

Local

Procedure

Step 1 Use the radio button and select **Local** as the authentication mode.

Step 2 Click **Apply** to confirm the authentication mode.

Radius

Procedure

Step 1 Use the radio button and select **Radius** as the authentication mode.

Note When using the DCNM AAA or Radius authentication, you should not specify the hash (#) symbol at the beginning of a secret key. Otherwise, DCNM will try to use # as encrypted, and it will fail.

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+

Procedure

Step 1 Use the radio button and select **TACACS+** as the authentication mode.

Note When using the DCNM AAA or Radius authentication, you should not specify the hash (#) symbol at the beginning of a secret key. Otherwise, DCNM will try to use **#** as encrypted, and it will fail.

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.

Note For IPv6 transport, enter Physical and VIP address for AAA authentication as the order of addresses changes during failover situation.

Step 4 Click **Apply** to confirm the authentication mode.

Switch

Procedure

Step 1 Use the radio button to select **Switch** as the authentication mode.

DCNM also supports LAN switches with the IPv6 management interface.

Step 2 Specify the Primary Switch name and click **Apply** to confirm the authentication mode.

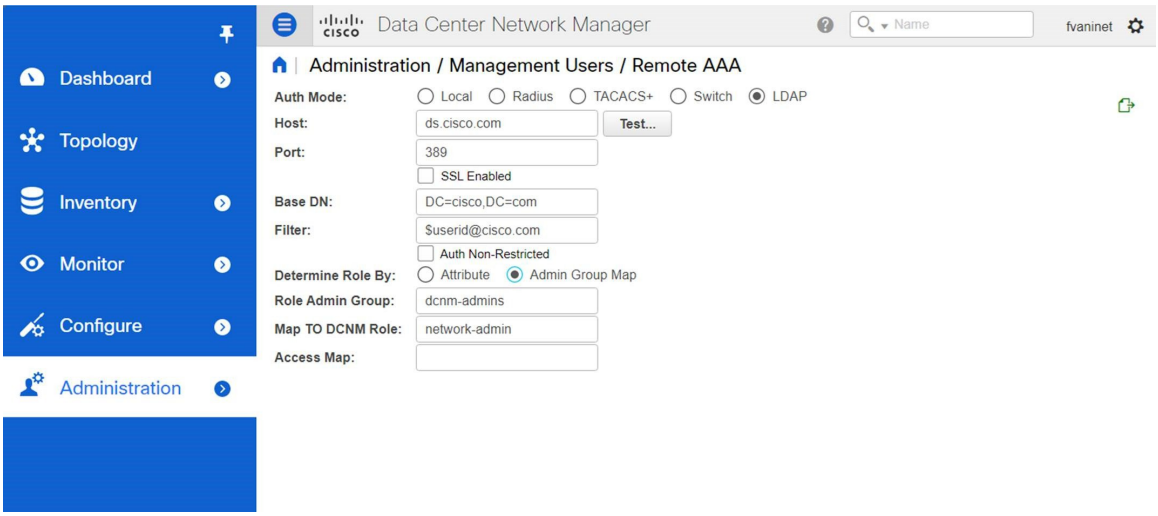
Step 3 (Optional) Specify the names for Secondary and Tertiary Switches.

Step 4 Click **Apply** to confirm the authentication mode.

LDAP

Procedure

Step 1 Use the radio button and select **LDAP** as the authentication mode.



Step 2 In the **Host** field, enter either the IPv4 or IPv6 address.

If DNS service is enabled, you can enter DNS address (hostname) of the LDAP server.

Step 3 In the **Port** field, enter a port number.

Enter 389 for non-SSL; enter 636 for SSL. By default, the port is configured for non-SSL.

Step 4 Select the **SSL Enabled** check box, if SSL is enabled on the AAA server.

Note You must enter **636** in the Port field, and select **SSL Enabled** check box to use LDAP over SSL.

This ensures the integrity and confidentiality of the transferred data by causing the LDAP client to establish a SSL session, before sending the bind or search request.

Note Cisco DCNM establishes a secured connection with the LDAP server using TLS. Cisco DCNM supports all versions of TLS. However, the specific version of TLS is determined by the LDAP server.

For example, if the LDAP server supports TLSv1.2 by default, DCNM will connect using TLSv1.2.

Step 5 In the **Base DN** field, enter the base domain name.

The LDAP server searches this domain. You can find the base DN by using the **dsquery.exe user -name**<*display_name*> command on the LDAP server.

For example:

```
ldapserver# dsquery.exe users -name "John Smith"

CN=john smith,CN=Users,DC=cisco,DC=com
```

The Base DN is DC=cisco,DC=com.

Note Ensure that you enter the elements within the Base DN in the correct order. This specifies the navigation of the application when querying Active Directory.

Step 6 In the **Filter** field, specify the filter parameters.

These values are used to send a search query to the Active Directory. The LDAP search filter string is limited to a maximum of 128 characters.

For example:

- $userid@cisco.com

  This matches the user principal name.

- CN=$userid,OU=Employees,OU=Cisco Users

  This matches the exact user DN.

Step 7 Choose an option to determine a role. Select either **Attribute** or **Admin Group Map**.

- **Admin Group Map**: In this mode, DCNM queries LDAP server for a user based on the Base DN and filter. If the user is a part of any user group, the DCNM role will be mapped to that user group.
- **Attribute**: In this mode, DCNM queries for a user attribute. You can select any attribute. When you choose **Attribute**, the **Role Admin Group** field changes to **Role Attributes**.

Step 8 Enter value for either **Roles Attributes** or **Role Admin Group** field, based on the selection in the previous step.

- If you chose **Admin Group Map**, enter the name of the admin group in the **Role Admin Group** field.
- If you chose **Attribute**, enter the appropriate attribute in the **Attributes** field.

Step 9 In the **Map to DCNM Role** field, enter the name of the DCNM role that will be mapped to the user.

Generally, **network-admin** or **network-operator** are the most typical roles.

For example:

```
Role Admin Group: dcnm-admins
Map to DCNM Role: network-admin
```

This example maps the Active Directory User Group **dcnm-admins** to the **network-admin** role.

To map multiple Active Directory User Groups to multiple roles, use the following format:

```
Role Admin Group:
Map To DCNM Role: dcnm-admins:network-admin;dcnm-operators:network-operator
```

Note that **Role Admin Group** is blank, and **Map To DCNM Role** contains two entries delimited by a semicolon.

Step 10 In the **Access Map** field, enter the Role Based Access Control (RBAC) device group to be mapped to the user.

Step 11 Click **Test** to verify the configuration. The Test AAA Server window appears.

Step 12 Enter a valid **Username** and **Password** in the Test AAA Server window.

If the configuration is correct, the following message is displayed.

```
Authentication succeeded.
The cisco-av-pair should return 'role=network-admin' if this user needs to
see the DCNM Admin pages. 'SME' roles will allow SME page access. All other
roles - even if defined on the switches - will be treated
as network operator.
```

This message is displayed regardless of 'Role Admin Group' or 'Attribute' mode. It implies that Cisco DCNM can query your Active Directory, the groups, and the roles are configured correctly.

If the test fails, the LDAP Authentication Failed message is displayed.

Warning Don't save the configuration unless the test is successful. You cannot access DCNM if you save incorrect configurations.

Step 13 Click **Apply Changes** icon (located in the right top corner of the screen) to save the configuration.

Step 14 Restart the DCNM SAN service.

- For Windows – On your system navigate to **Computer Management > Services and Applications > Services**. Locate and right click on the DCNM application. Select **Stop**. After a minute, right click on the DCNM application and select **Start** to restart the DCNM SAN service.
- For Linux – Go to **/etc/init.d/FMServer.restart** and hit return key to restart DCNM SAN service.

Managing Local Users

As an admin user, you can use Cisco DCNM Web UI to create a new user, assign the role and associate one or more groups or scope for the user.

This section contains the following:

Adding Local Users

Procedure

Step 1 From the menu bar, choose **Administration > Management Users > Local**. You see the **Local Users** page.

Step 2 Click **Add User**.

You see the **Add User** dialog box.

Step 3 Enter the username in the **User name** field.

Note The username is case sensitive, but the username guest is a reserved name, which is not case sensitive. 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.

Note All special characters, except SPACE is allowed in 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.

Deleting Local Users

To delete local users from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > Management Users > Local**.

The **Local Users** page is displayed.

Step 2 Select one or more users from the **Local Users** table and click the **Delete User** button.

Step 3 Click **Yes** on the warning window to delete the local user. Click **No** to cancel deletion.

Editing a User

To edit a user from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > Management Users > Local**.

Step 2 Use the checkbox to select a user and click the **Edit User** icon.

Step 3 In the **Edit User** window, the **Username** and **Role** are mentioned by default. Specify the **Password** and **Confirm Password**.

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

User Access

You can select specific groups or fabrics that local users can access. This restricts local users from accessing specific groups or fabrics for which they have not been provided access. To do this, perform the following steps:

Procedure

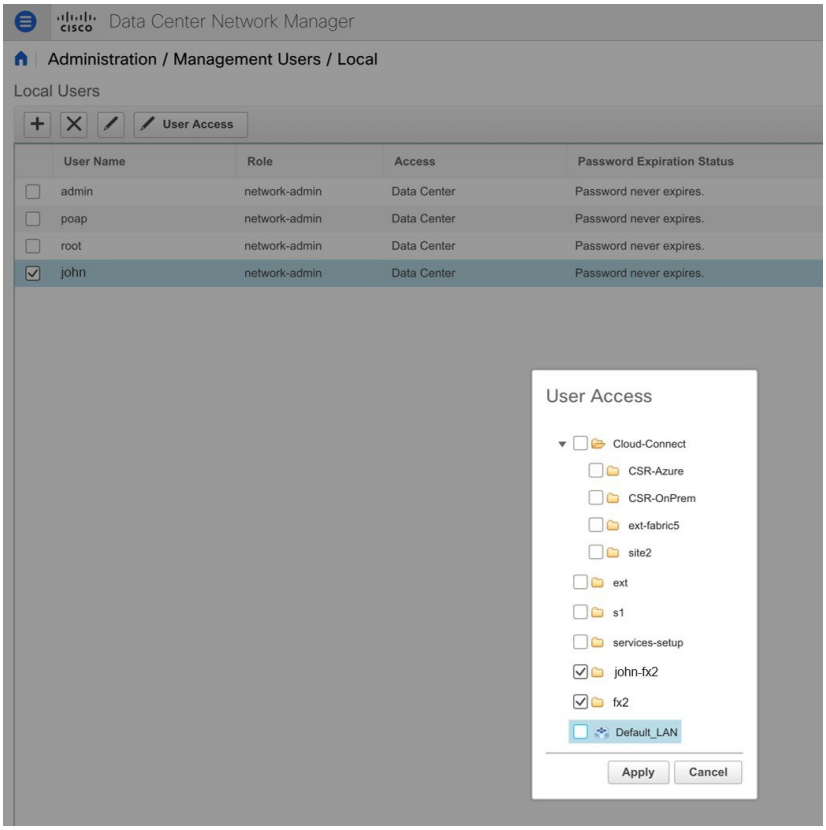
Step 1 Choose **Administration > Management Users > Local**.

The **Local Users** window is displayed.

Step 2 Select one user from the **Local Users** table. Click **User Access**.

The **User Access** selection window is displayed.

Step 3 Select the specific groups or fabrics that the user can access and click **Apply**.



Managing Clients

You can use Cisco DCNM to disconnect DCNM Client Servers.

Procedure

Step 1 Choose **Administration > Management Users > Clients**.

A list of DCNM Servers are displayed.

Step 2 Use the check box to select a DCNM server and click **Disconnect Client** to disconnect the DCNM server.

Note You cannot disconnect a current client session.

Performance Setup

The Performance Setup menu includes the following submenus:

Performance Setup LAN 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 DCNM to add and remove performance collections. License the switch and kept it in the **Managed Continuously** state before creating a collection for the switch.



Note To collect Performance Manager data, ICMP ping must be enabled between the switch and DCNM server. Set **pm.skip.checkPingAndManageable** server property to true and then restart the DCNM. Choose Web **UI** > **Administration** > **DCNM Server** > **Server Properties** to set the server property.

To add a collection, follow these steps:

Procedure

Step 1 Choose **Administration > Performance Setup > LAN Collections**.

Step 2 For all the licensed LAN switches, use the check boxes to enable performance data collection for **Trunks**, **Access**, **Errors & Discards**, and **Temperature Sensor**.

Step 3 Use the check boxes to select the types of LAN switches for which you want to collect performance data.

Step 4 Click **Apply** to save the configuration.

Step 5 In the confirmation dialog box, click **Yes** to restart the Performance Manager. The Performance Manager has to be restarted for any new setting to take effect.

Performance Setup Thresholds

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 DCNM to add and remove performance collections. License the switch and keep it in the **Managed Continuously** state before creating a collection for the switch.

Procedure

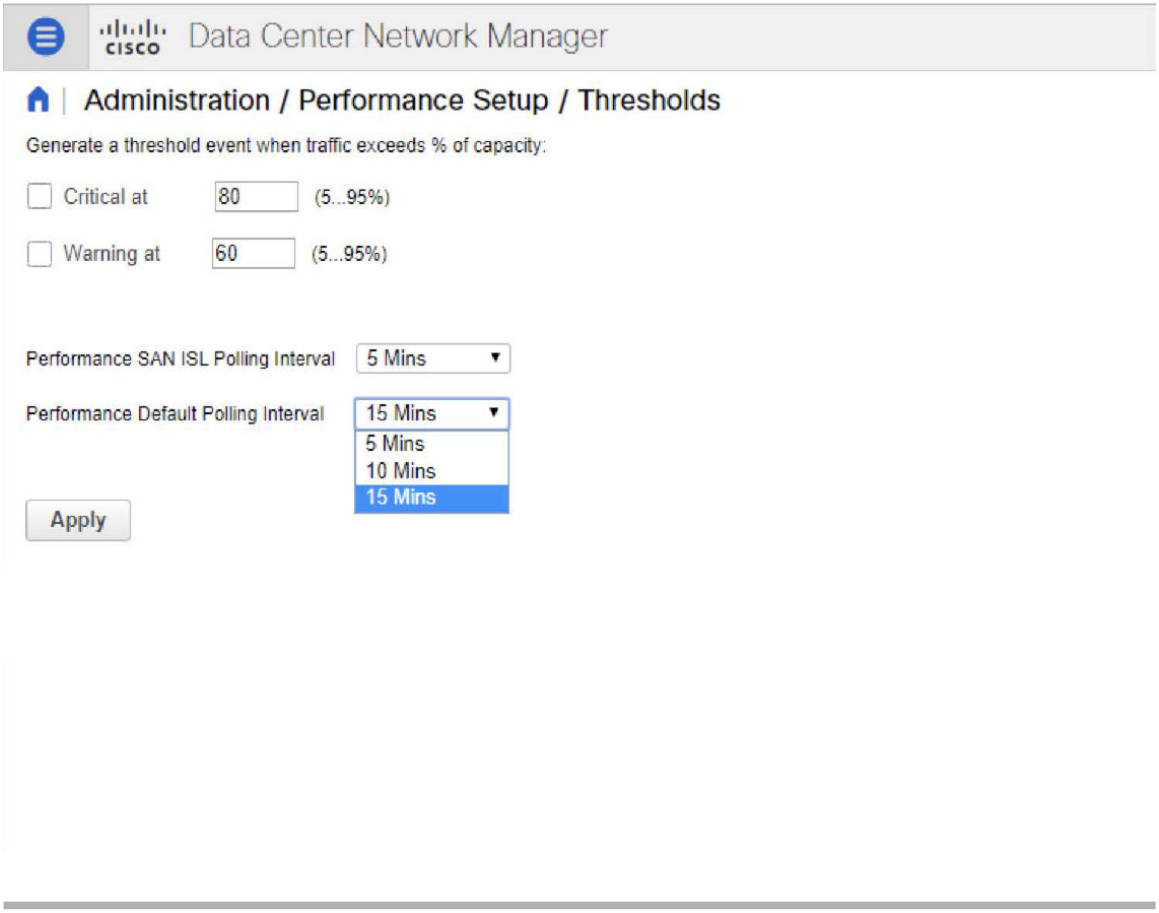
Step 1 Choose **Administration > Performance Setup > Thresholds**.

Step 2 Under **Generate a threshold event when traffic exceeds % of capacity**, use the check box to specify the **Critical at** and **Warning at** values. The range for **Critical at** is from 5 to 95, and the default is 80. The range for **Warning at** is from 5 to 95, and the default is 60.

Step 3 Select a value for **Performance SAN ISL Polling Interval** from the drop-down list. Valid values are **5 Mins**, **4 Mins**, **3 Mins**, **2 Mins**, **1 Min**, and **30 Sec**. The default is **30 Sec**.

Step 4 Select a value for **Performance Default Polling Interval** from the drop-down list. Valid values are **5 Mins** , **10 Mins**, and **15 mins**. The default value is **5 Mins**.

Step 5 Click **Apply**.



Event Setup

The Event Setup menu includes the following submenus:

Viewing Events Registration

To enable **Send Syslog**, **Send Traps** and **Delayed Traps** you must configure the following in the DCNM SAN client:

- Enabling **Send Syslog**: Choose **Physical Attributes** > **Events** > **Syslog** > **Servers**. Click **Create Row**, provide the required details, and click **Create**.
- Enabling **Send Traps**: Choose **Physical Attributes** > **Events** > **SNMP Traps** > **Destination**. Click **Create Row**, provide the required details, and click **Create**.
- Enabling **Delayed Traps**: Choose **Physical Attributes** > **Events** > **SNMP Traps** > **Delayed Traps**. In the **Feature Enable** column, use the check boxes to enable delayed traps for the switch and specify the delay in minutes.

Procedure

Step 1 Choose **Administration > Event Setup > Registration**.

The SNMP and Syslog receivers along with the statistics information are displayed.

Step 2 Check the **Enable Syslog Receiver** check box and click **Apply**, to enable the syslog receiver if it is disabled in the server property.

To configure event registration or syslog properties, choose **Administration > DCNM Server > 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 selected, the events will not be displayed in the events page of the Web client.

The columns in the second table display the following:

- Switches sending traps
- Switches sending syslog
- Switches sending syslog accounting
- Switches sending delayed traps

Notification Forwarding

You can use Cisco DCNM Web UI to add and remove notification forwarding for system messages.

This section contains the following:

Adding Notification Forwarding

Cisco DCNM Web UI forwards fabric events through email or SNMPv1 traps.

To add and remove notification forwarding for system messages from the Cisco DCNM Web UI, perform the following steps:



Note Test forwarding works only for the licensed fabrics.

Procedure

Step 1 Choose **Administration > Event Setup > Forwarding**.

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 2 Check the **Enable** checkbox to enable events forwarding.

Step 3 Specify the **SMTP Server** details and the **From** email address.

Step 4 Click **Apply** to save the configuration, or in the **Apply and Test** icon, use the drop-down to select the fabric.

Click **Apply and Test** to save and test the configuration.

Step 5 In the **Event Count Filter**, add a filter for the event count to the event forwarder.

The forwarding stops forwarding an event if the event count exceeds the limit as specified in the event count filter. In this field, you can specify a count limit. Before an event can be forwarded, the Cisco DCNM checks if its occurrence exceeds the count limit. If it does, the event will not be forwarded.

Step 6 Select the **Snooze** checkbox and specify the **Start** date and time and the **End** date and time. Click **Apply** to save the configuration.

Step 7 Under the **Event Forwarder Rules** table, click the **+** icon to add an event forwarder rule.

You see the **Add Event Forwarder Rule** dialog box.

Step 8 In the **Forwarding Method**, choose either **E-mail** or **Trap**. If you choose **Trap**, a **Port** field is added to the dialog box.

Step 9 If you choose the **E-mail** forwarding method, enter the IP address in the **Email Address** field. If you choose the **Trap** method, enter the trap receiver IP address in the **Address** field and specify the port number.

You can either enter an IPv4 or IPv6 addresses or DNS server name in the **Address** field.

Step 10 For **Forwarding Scope**, choose the **Fabric/LAN** or **Port Groups** for notification.

Step 11 In the **Source** field, select **DCNM** or **Syslog**.

If you select **DCNM**, then:

a) From the **Type** drop-down list, choose an event type.
b) Check the **Storage Ports Only** check box to select only the storage ports.
c) From the **Minimum Severity** drop-down list, select the severity level of the messages to receive.
d) Click **Add** to add the notification.

If you select **Syslog**, then:

a) In the **Facility** list, select the syslog facility.
b) Specify the syslog **Type**.
c) In the **Description Regex** field, specify a description that matches with the event description.
d) From the **Minimum Severity** drop-down list, select the severity level of the messages to receive.
e) Click **Add** to add the notification.

Note The **Minimum Severity** option is available only if the **Event Type** is set to All.

The traps that are transmitted by Cisco DCNM correspond to the severity type. A text description is also provided with the severity type.

```
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.

Procedure

Step 1 Choose **Administration > Event Setup > Forwarding**.

Step 2 Select the check box in front of the notification that you want to remove and click **Delete**.

Event Suppression

Cisco DCNM allows you to suppress the specified events that are based on the user-specified suppressor rules. Such events will not be displayed on the Cisco DCNM Web UI. The events will neither be persisted to DCNM database, nor forwarded via email or 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.



Note You cannot suppress EMC Call Home events from the Cisco DCNM Web UI.

This section includes the following:

Add Event Suppression Rules

To add rules to the Event Suppression from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > Event Setup > Suppression**.

The **Suppression** window is displayed.

Step 2 Click the **Add** icon above the **Event Suppressors** table.

The **Add Event Suppressor Rule** window is displayed.

Step 3 In the **Add Event Suppressor Rule** window, specify the **Name** for the rule.

Step 4 Select the required **Scope** for the rule that is based on the event source.

In the Scope drop-down list, the LAN groups and the port groups are listed separately. You can choose **LAN, Port Groups** or **Any**. For **LAN**, select the scope of the event at the Fabric or Group or Switch level. You can only select groups for **Port Group** scope. If use selects **Any** as the scope, the suppressor rule is applied globally.

Step 5 Enter the **Facility** name or choose from the **LAN Switch Event Facility** List.

If you do not specify a facility, wildcard is applied.

Step 6 From the drop-down list, select the Event **Type**.

If you do not specify the event type, wildcard is applied.

Step 7 In the **Description Matching** field, specify a matching string or regular expression.

The rule matching engine uses regular expression that is supported by Java Pattern class to find a match against an event description text.

Step 8 Check the **Active Between** box and select a valid time range during which the event is suppressed.

By default, the time range is not enabled, i.e., the rule is always active.

Note In general, you must not suppress accounting events. Suppressor rule for Accounting events can 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 the password synchronization between DCNM and managed switches. To suppress Accounting events, navigate to the **Suppressor table** and invoke the **Add Event Suppressor Rule** dialog window.

Note Choose **Monitor > Switch > Events** to create a suppressor rule for a known event. There is no such shortcut to create suppressor rules for Accounting events.

Delete Event Suppression Rule

To delete event suppressor rules from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > Event Setup > 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:

Procedure

Step 1 Choose **Administration > Event Setup > Suppression**.

Step 2 Select the rule from the list and click **Edit**.

You can edit **Facility**, **Type**, **Description Matching** string, and **Valid time range**.

Step 3 Click **Apply** to save the changes,

Credentials Management

The Credential Management menu includes the following submenus:

LAN Credentials

While changing the device configuration, Cisco DCNM uses the device credentials provided by you. However, if the LAN Switch credentials are not provided, Cisco DCNM prompts you to open the **Administration > Credentials Management > LAN Credentials** page to configure LAN credentials.

Cisco DCNM uses two sets of credentials to connect to the LAN devices:

- **Discovery Credentials**—Cisco DCNM uses these credentials during discovery and periodic polling of the devices.
- **Configuration Change Credentials**—Cisco DCNM uses these credentials when user tries to use the features that change the device configuration.

LAN Credentials Management allows you to specify configuration change credentials. Before changing any LAN switch configuration, you must furnish *Configuration Change* SSH credentials for the switch. If you do not provide the credentials, the configuration change action will be rejected.

These features get the device write credentials from LAN Credentials feature.

- Upgrade (ISSU)
- Maintenance Mode (GIR)
- Patch (SMU)
- Template Deployment
- POAP-Write erase reload, Rollback
- Interface Creation/Deletion/Configuration
- VLAN Creation/Deletion/Configuration
- VPC Wizard

You must specify the configuration change credentials irrespective of whether the devices were discovered initially or not. This is a one-time operation. Once the credentials are set, that will be used for any configuration change operation.

Default Credentials

Default credentials is used to connect all the devices that the user has access to. You can override the default credentials by specifying credentials for each of the devices in the Switch Table below.

Cisco DCNM tries to use individual switch credentials in the Switch Table, to begin with. If the credentials (username/password) columns are empty in the Switch Table, the default credentials will be used.

Switch Table

Switch table lists all the LAN switches that user has access. You can specify the switch credentials individually, that will override the default credentials. In most cases, you need to provide only the default credentials.

You can perform the following operations on this screen.

- Edit Credentials, on page 234
- Validate Credentials, on page 234
- Clear Switch Credentials, on page 234
- Credentials Management with Remote Access, on page 235

The LAN Credentials for the DCNM User table has the following fields.

Field	Description
Switch	Displays the LAN switch name.
IP Address	Specifies the IP Address of the switch.
User Name	Specifies the username of the switch DCNM user.
Password	Displays the encrypted form of the SSH password.
Group	Displays the group to which the switch belongs.

Edit Credentials

Perform the following task to edit the credentials.

1. From the Cisco DCNM home page, choose **Administration > Credentials Management > LAN Credentials**, check the **Switch** check box for which you need to edit the credentials.
2. Click Edit icon.
3. Specify **User Name** and **Password** for the switch.

Validate Credentials

Perform the following task to validate the credentials.

1. From the **Administration > Credentials Management > LAN Credentials**, check the **Switch** check box for which you need to validate the credentials.
2. Click **Validate**.

   A confirmation message appears, stating if the operation was successful or a failure.

Clear Switch Credentials

Perform the following task to clear the switch credentials.

1. From the **Administration > Credentials Management > LAN Credentials**, check the **Switch** check box for which you need to clear the credentials.

2. Click **Clear**.
3. Click **Yes** to clear the switch credentials from the DCNM server.

Credentials Management with Remote Access

DCNM allows you to authenticate users in different modes such as:

- Local Users - In this mode, you can use the Cisco DCNM Web UI to create a new user, assign a role, and provide access to one or more fabrics or groups for the user.
- Remote Users - In this mode, you can log in to DCNM. The DCNM server fetches information from the Remote Authentication server, for example, the Cisco Identity Services Engine (ISE), for AAA authentication. Cisco supports TACACS+, RADIUS, and LDAP options for remote authentication. For more information, see Remote AAA.

When you configure DCNM for remote authentication, the AAA server handles both authentication and authorization. DCNM forwards the entered user login and password to the AAA server to check for authentication. Post authentication, the AAA server returns the appropriate privileges/role assigned to the user through the **cisco-avpair** attribute. This attribute can contain the list of fabrics that a particular user can access. The supported roles for DCNM LAN deployments are as follows:

- network-admin
- network-operator

Both device discovery credentials and LAN credentials provide write access to the devices, but they differ—as the write operation is performed only with LAN credentials. Device discovery credentials are associated with each device and entered only once, that is, when you import the device into DCNM. DCNM uses these credentials for periodic rediscovery using a mix of SSH and SNMPv3 access to the device. However, LAN credentials are configured for every user on a per-user basis. If a user with an appropriate role has access to DCNM, then that user can enter the LAN credentials to get write access to the devices. The write operations use the LAN credentials to access the device, which allows for an appropriate audit trail of the changes made in DCNM by every user and the resultant changes in the device.

When you configure DCNM using Remote Authentication Methods such as TACACS+ or RADIUS, the users can set their LAN credentials as follows:

- Regular AAA Remote Authentication
- AAA Remote Authentication Passthrough Mechanism
- AAA Remote Authentication Using DCNM Service Account

Regular AAA Remote Authentication

Post authentication, when a user with an appropriate role logs in to DCNM for the first time, DCNM prompts the user to enter the LAN credentials. As mentioned earlier, DCNM uses these credentials to provide write access to the devices. All users must follow this process. Consider that an internal business policy requires the users to change password every 3-6 months. Then all the users must update their passwords for device access in the DCNM **LAN Credentials** window. Also, they must update their passwords in the AAA server.

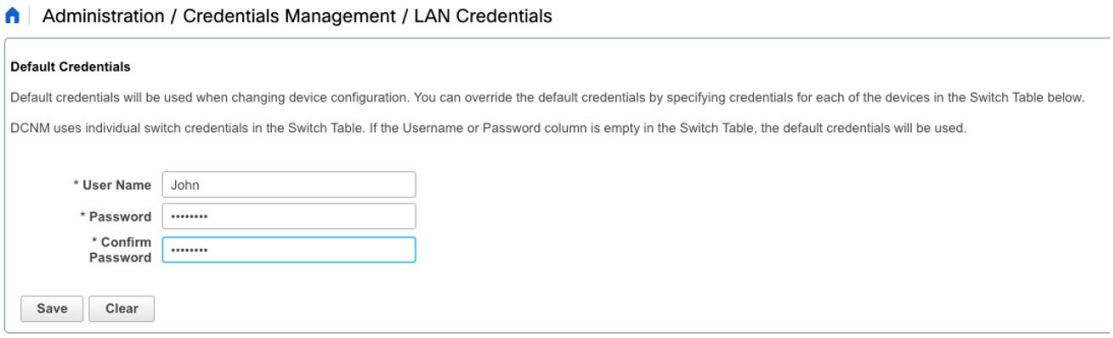
For example, let us consider a user named John, who has authentication on the ISE server.

1. John logs in to DCNM with his user credentials.

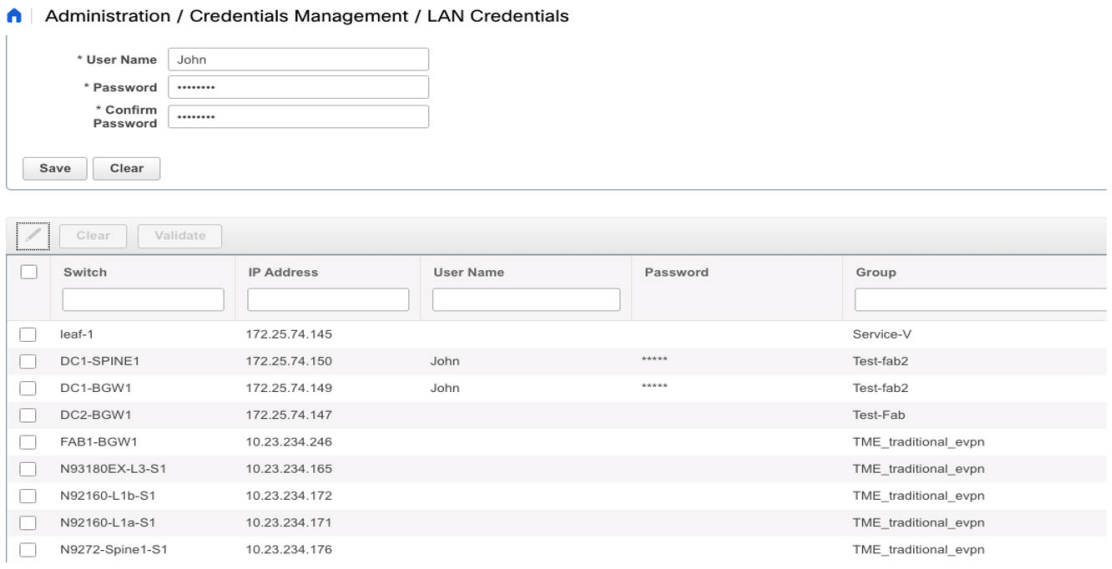
2. The ISE server authenticates the user credentials of John, and DCNM displays a message to enter his LAN switch credentials. DCNM uses these credentials to perform various configurations and write operations on the devices.



3. John enters his LAN switch credentials. DCNM uses the LAN switch credentials for all write operations triggered by John on all devices. However, John can also opt to enter LAN switch credentials on a per-device access basis. This per-device access option overrides the access provided by entering the default credentials.



When John logs in to DCNM again, DCNM doesn't display any message to enter the LAN switch credentials as it has already captured his LAN switch credentials. John uses the same credentials to log in to DCNM and to the devices that he can access.



4. Now, consider that after a few months, the Corporate IT policy changes. Then John must update his password in the Remote AAA server, and also perform Step 3 to allow DCNM to update his LAN switch credentials.

Thus, in this mode, when John logs in to the DCNM Web GUI with his updated password, DCNM doesn't display any message to enter LAN credentials. However, John must update the password in LAN Credentials. Updating the password is necessary as it allows DCNM to inherit the newly updated password and perform write operations on the devices.

AAA Remote Authentication Passthrough Mechanism

In this mode, when a user enters the username and password to log in to DCNM, DCNM automatically copies the user credentials to the Default Credentials in the LAN switch credentials settings for that user. As a result, when the user logs in for the first time, DCNM doesn't display the message to enter the LAN switch credentials.

1. Use SSH to log in to DCNM as a sysadmin user.
2. Log in to the `/root/directory` using the **su** command.
3. Navigate to the `/usr/local/cisco/dcm/fm/conf/server.properties` file.
4. Add the following server property to the file and save the changes.

   dcnm.lanSwitch.sameUserAccount=true

```
[root@dcnm sysadmin]# cat /usr/local/cisco/dcm/fm/conf/server.properties | grep dcnm.lan
dcnm.lanSwitch.sameUserAccount=true
[root@dcnm sysadmin]#
```

5. Restart DCNM using the **service FMServer restart** command.
6. Now, John logs in to DCNM.
7. After successful authentication, DCNM doesn't display the message to update the LAN switch credentials, as it automatically copies this information to the LAN switch credentials.
8. Consider that after a few months, the Corporate IT policy changes. In this mode, John must update his password in the Remote AAA server. After that, when John logs in to DCNM, DCNM automatically copies the updated credentials to the Default LAN Credentials associated with the user John.

AAA Remote Authentication Using DCNM Service Account

Often, the customers prefer to track all the changes made from the DCNM controller with a common service account. In the following example, a user makes changes using the DCNM controller, which results in changes on the device. These changes are audit logged on the device, against a common service account. Thus, it is possible to distinguish the controller-triggered changes from other changes (also known as Out-of-Band changes) made by the user directly on the device. The Out-of-Band changes appear in the device accounting logs as made from the user account.

For example, create a service account with the name **Robot** on the remote AAA server. Using the corresponding credentials, the Robot user can log in to DCNM. The Robot user can enter the default LAN credentials to have write access to the devices. The DCNM network-admin enables a server property that automatically sets the default LAN credentials for all the users and inherits the default LAN credentials associated with Robot.

Therefore, when any user logs in to DCNM and makes any configuration changes, DCNM pushes the changes to the devices using the LAN credentials of Robot. The DCNM deployment history logs track the user who

triggered the change and display the corresponding changes deployed from DCNM to the switch in the audit log with the user Robot.

To set up the service account on the DCNM, perform the following steps:

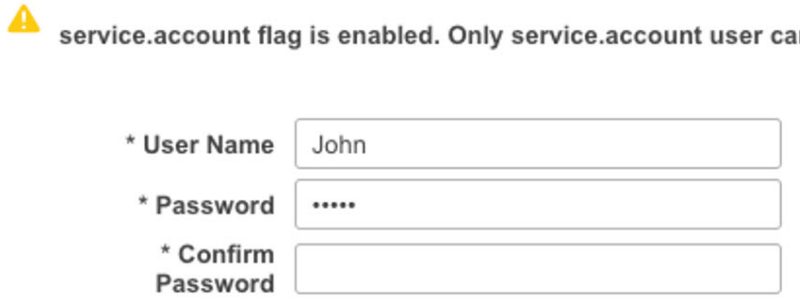
1. Use SSH to log in to DCNM as a sysadmin user.
2. Log in to the `/root/ directory` using the **su** command.
3. Navigate to the `/usr/local/cisco/dcm/fm/conf/server.properties` file.
4. Add the following server property to the file and save the changes.

   service.account=robot

   Note You can enable either an AAA passthrough account or a Service Account.

```
[root@dcnm sysadmin]# cat /usr/local/cisco/dcm/fm/conf/server.properties | grep robot
service.account=robot
[root@dcnm sysadmin]#
```

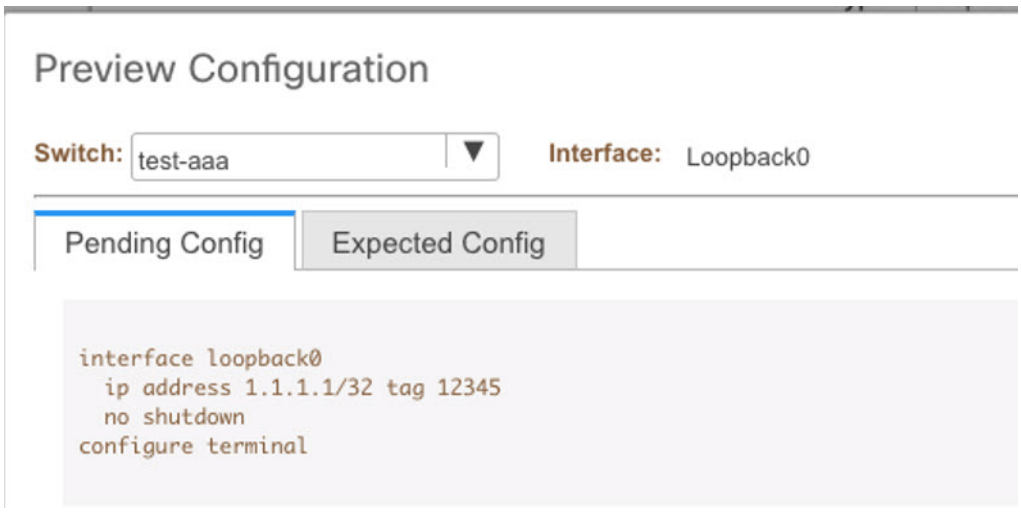
5. Restart DCNM using the **service FMServer restart** command.
6. Now, John logs in to DCNM.
7. After successful authentication, DCNM doesn't display the message to update the LAN switch credentials. However, when John navigates to the **LAN Credentials** page, DCNM displays a message stating that the Service Account is enabled in DCNM and, hence, all LAN credentials will be inherited from the service account.



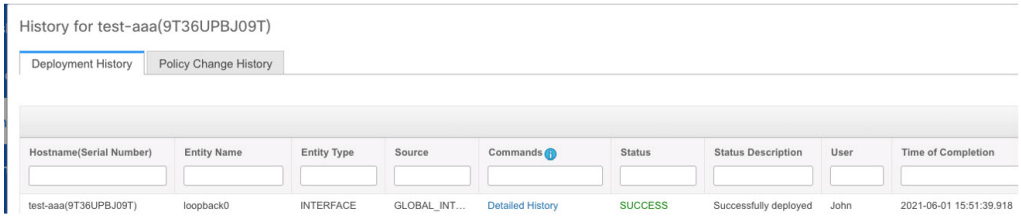
Service Account Configuration Audit

The following workflow example allows for verification of the configuration audit while using the DCNM service account feature. However, you must have completed the Service Account Activation procedure.

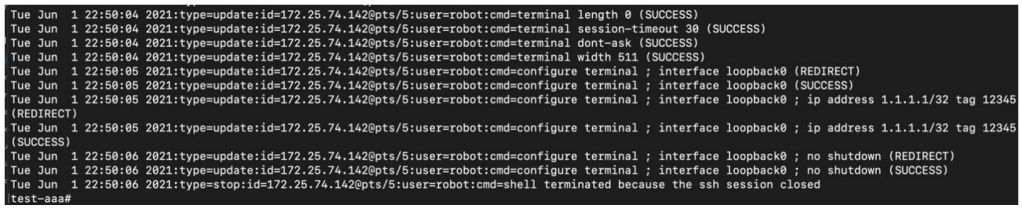
1. John creates a test loopback on a device.

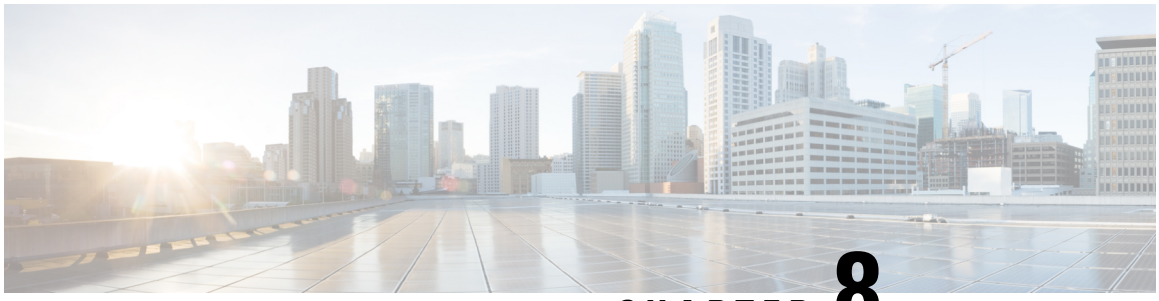


2. John deploys the configuration using DCNM.
3. The DCNM Deployment history confirms that John made the recent configuration change.



4. The accounting logs of the device indicate that the DCNM Service Account (that is, Robot, in this example) has triggered the changes on the NX-OS device.





CHAPTER 8

Applications

Cisco Data Center Network Manager (DCNM) uses the application framework to host various plugins and microservices to support operations and related features in Cisco DCNM.

The Applications Framework provides the following features:

- An infrastructure for hosting applications that require more system resources as the scale of the network increases.
- An independent application development-deployment-management lifecycle for applications.

Cisco DCNM Applications Framework supports two modes namely clustered mode and unclustered mode. In clustered mode, the compute nodes are clustered together whereas in the latter only the DCNM server nodes namely the active/standby exist. Most of the applications for ex: Network Insights require clustered setup to be ready before they can be uploaded and deployed using DCNM Applications Framework.

- Cisco DCNM in Unclustered Mode, on page 241
- Cisco DCNM in Clustered Mode, on page 242
- Installing and Deploying Applications, on page 253
- Application Framework User Interface, on page 256
- Catalog, on page 257
- Compute, on page 265
- Preferences, on page 267
- Failure Scenario, on page 267

Cisco DCNM in Unclustered Mode

From Cisco DCNM Release 11.0(1), the unclustered mode is the default deployment mode in both Standalone and Native HA environment. In this mode, the Cisco DCNM runs some of its internal services as containers, also.

- Endpoint Locator is running as a container application, from Cisco DCNM Release 11.1(1).
- Configuration Compliance service is a container application, from Cisco DCNM Release 11.0(1).
- Virtual Machine Manager (VMM) is also a container application, from Cisco DCNM Release 11.0(1)

Cisco DCNM leverages resources from the Standby node for running some containers applications. The Cisco DCNM Active and Standby nodes work together to extend resources to the overall functionality and deployment

of DCNM and its applications. However, it has limited resources to run some of the advanced applications and to extend the system to deploy more applications delivered through the Cisco AppCenter. For example, you cannot deploy the Network Insights applications that are downloaded from the Cisco AppCenter, for production, in unclustered mode.

To install and deploy applications, see Installing and Deploying Applications, on page 253.

For best practices and recommended deployments for IP address configurations of all interfaces of the Cisco DCNM and Compute nodes, see *Best Practices for Deploying Cisco DCNM and Computes* in *Cisco DCNM Installation Guide*, for your deployment type.

Cisco DCNM in Clustered Mode

By default, the clustered mode if not enabled on the Cisco DCNM deployments. Enable the cluster mode after you deploy the Cisco DCNM Server. In a clustered mode, the Cisco DCNM Server with more compute nodes provides an architecture to expand resources, as you deploy more applications.

Compute nodes are scale out application hosting nodes that run resource-intensive services to provide services to the larger Fabric. When compute nodes are added, all services that are containers, run only on these nodes. This includes Config Compliance, Endpoint Locator, and Virtual Machine Manager. The Elasticsearch time series database for these features runs on compute nodes in clustered mode. In the clustered mode deployment, the DCNM Servers do not run containerized applications. All applications that work in unclustered mode works in the clustered mode, also.



Note The clustered mode is not supported on Cisco DCNM for Media Controller deployment.

From Cisco DCNM Release 11.1(1), in a Native HA setup, 80 switches with Endpoint Locator, Virtual Machine Manager, config compliance are validated in the unclustered mode. For a network exceeding 80 switches, with these features in a given Cisco DCNM instance (maximum qualified scale is 256 switches), we recommend that you enable clustered mode.

While the Cisco DCNM core functionalities only run on the Native HA nodes, addition of compute nodes beyond 80 switches is to build a scale-out model for Cisco DCNM and related services.

From Release 11.2(1), you can configure IPv6 address for Network Management for compute clusters. However, DCNM does not support IPv6-address for containers, and must connect to DCNM using only IPv4 address only.

For best practices and recommended deployments for IP address configurations of all interfaces of the Cisco DCNM and Compute nodes, see *Best Practices for Deploying Cisco DCNM and Computes* in *Cisco DCNM Installation Guide*, for your deployment type.

Requirements for Cisco DCNM Clustered Mode



Note We recommend that you install the Cisco DCNM in the Native HA mode.

Cisco DCNM LAN Fabric Deployment Without Network Insights (NI)

Note For information about various system requirements for proper functioning of Cisco DCNM LAN Fabric deployment, see .

Refer to *Network Insights User guide* for sizing information for Cisco DCNM LAN Deployment with Network Insights (NI).

To see the verified scale limits for Cisco DCNM 11.4(1) for managing LAN Fabric deployments, see .

Table 44: Upto 80 Switches

Node	CPU Deployment Mode	CPU	Memory	Storage	Network
DCNM	OVA/ISO	16 vCPUs	32G	500G HDD	3xNIC
Computes	NA	—	—	—	—

Table 45: 81–250 Switches

Node	CPU Deployment Mode	CPU	Memory	Storage	Network
DCNM	OVA/ISO	16 vCPUs	32G	500G HDD	3xNIC
Computes	OVA/ISO	16 vCPUs	64G	500G HDD	3xNIC

Cisco DCNM LAN Deployment with NIA and NIR Software Telemetry

Note We recommend that you install the Cisco DCNM in the Native HA mode.

Table 46: Upto 80 Switches

Node	CPU Deployment Mode	CPU	Memory	Storage	Network
DCNM	OVA/ISO	16 vCPUs	32G	500G HDD	3xNIC
Computes x 3	OVA/ISO	16 vCPUs	64G	500G HDD	3xNIC

Table 47: 81–250 Switches

Node	CPU Deployment Mode	CPU	Memory	Storage	Network
DCNM	OVA/ISO	16 vCPUs	32G	500G HDD	3xNIC
Computes x 3	ISO	32 vCPUs	256G	2.4-TB HDD	3xNIC[1]

[1] Network card: Quad-port 10/25G

Subnet Requirements

In general, Eth0 of the Cisco DCNM server is used for Management, Eth1 is used to connect Cisco DCNM Out-Of-Band with switch management, and eth2 is used for In-Band front panel connectivity of Cisco DCNM. The same concept extends into compute nodes as well. Some services in clustered mode have other requirements. Some services require a switch to reach into Cisco DCNM. For example, Route Reflector to Endpoint Locator connection or switch streaming telemetry into the Telemetry receiver service of the application require a switch to reach DCNM. This IP address needs to remain sticky during all failure scenarios. For this purpose, an IP pool must be provided to Cisco DCNM at the time of cluster configuration for both out-of-band and In-Band subnets.

Telemetry NTP Requirements

For telemetry to work correctly, the Cisco Nexus 9000 switches and Cisco DCNM must be time that is synchronized. Cisco DCNM telemetry manager does the required NTP configuration as part of enablement. If there is a use-case to change the NTP server configuration manually on the switches ensure that the DCNM and the switches are time synchronized, always. To set up telemetry network configuration, see .

Installing a Cisco DCNM Compute

Note With Native HA installations, ensure that the HA status is **OK** before DCNM is converted to cluster mode.

A Cisco DCNM Compute can be installed using an ISO or OVA of a regular Cisco DCNM image. It can be deployed directly on a bare metal using an ISO or a VM using the OVA. After you deploy Cisco DCNM, using the DCNM web installer, choose **Compute** as the install mode for Cisco DCNM Compute nodes. On a Compute VM, you will not find DCNM processes or postgres database; it runs a minimum set of services that are required to provision and monitor applications.

Networking Policies for OVA Installation

For each compute OVA installation, ensure that the following networking policies are applied for the corresponding vSwitches of host:

- Log on to the vCenter.
- Click on the Host on which the computes OVA is running.
- Click **Configuration** > **Networking**.

- Right click on the port groups corresponding to the eth1 and eth2, and select **Edit Settings**.

  The **VM Network - Edit Settings** is displayed.

- In Security settings, for **Promiscuous** mode, select **Accepted**.
- If a DVS Port-group is attached to the compute VM, configure these settings on the **vCenter > Networking > Port-Group**. If a normal vSwitch port-group is used, configure these settings on **Configuration > Networking > port-group** on each of the Compute's hosts.

Figure 1: Security Settings for vSwitch Port-Group

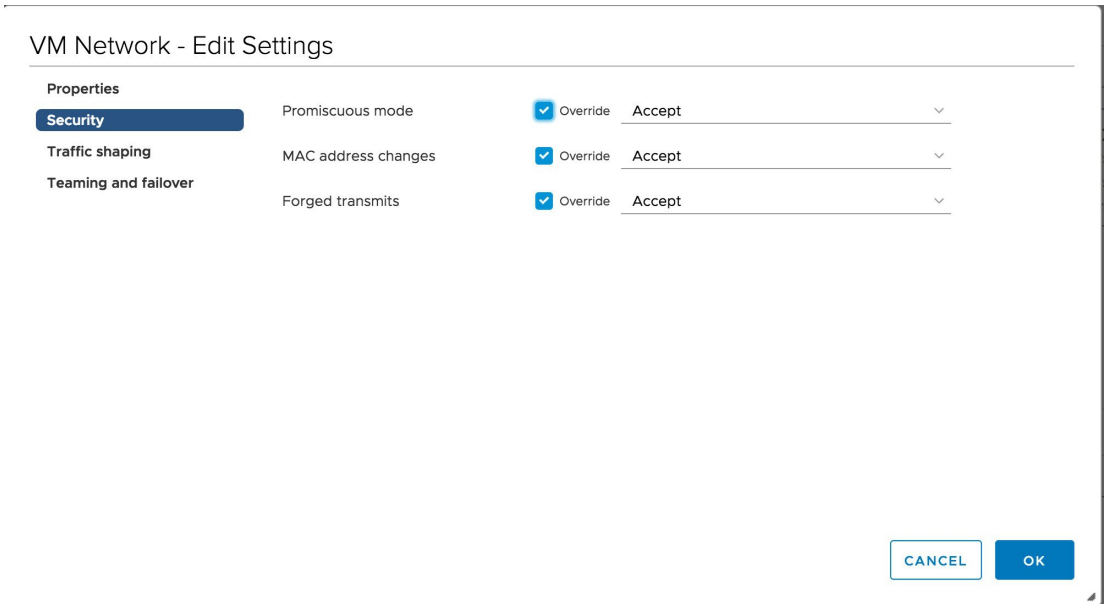
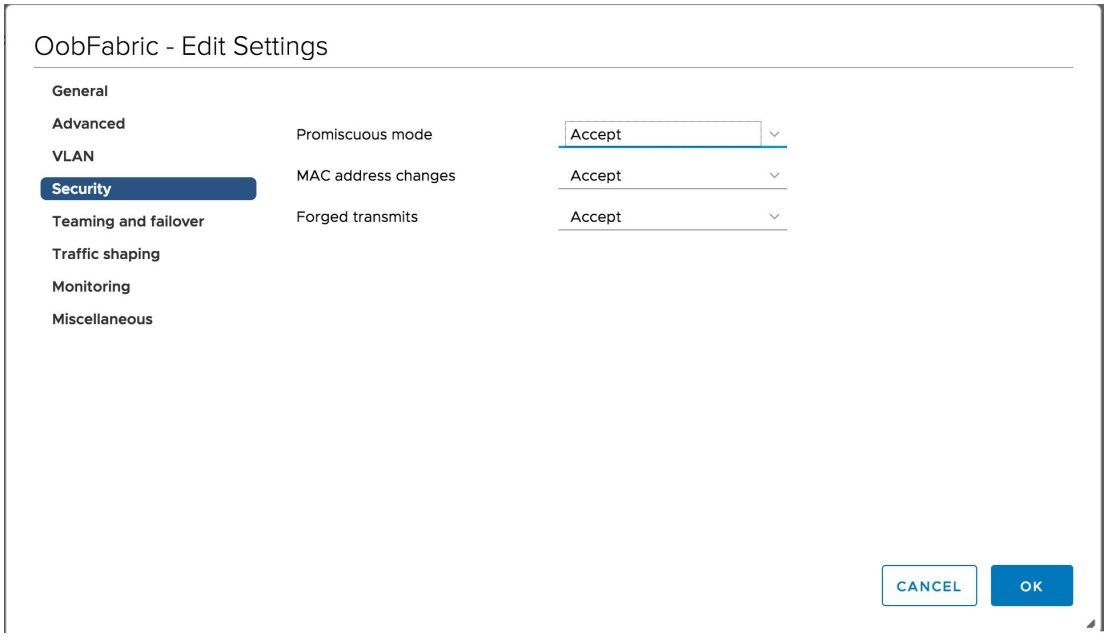


Figure 2: Security Settings for DVSwitch Port-Group



Note Ensure that you repeat this procedure on all the hosts, where a Compute OVA is running.

Enabling the Compute Cluster

Note Ensure that you enable Compute Cluster before you install applications. The applications that are installed via the AppCenter will not work if you enable the compute cluster after installing the applications.

Note The services are down until the configuration is complete. Ensure that the session is active while configuration is in progress.

Note If you enable clustered mode while installing Cisco DCNM, you don't need to enable cluster. The compute nodes will be discovered on Cisco DCNM **Web UI > Applications > Compute**. Go to Compute, on page 265 to form a cluster.

If you did not enable clustered mode while installation, use the following command to enable the compute cluster.

appmgr afw config-cluster
[--ewpool<*InterApp-Subnet*>*]***--oobpool**<*OutOfBand-Subnet*>**--ibpool**<*Inband-Subnet*>**--computeip**<*compute-ip*>

Where:

- **ewpool**: specifies the east-west pool subnet; for inter-service connectivity.

  This field is optional, if the inter-application subnet is specified during Cisco DCNM installation for your deployment type. These addresses are not used directly between the computes, or to communicate with another node. These are used by containers to communicate with each other. This subnet must be minimum of /24 (256 addresses) and a maximum of a /20 (4096 addresses).

  This field is optional if the Inter-app subnet is specified during Cisco DCNM deployment installation.

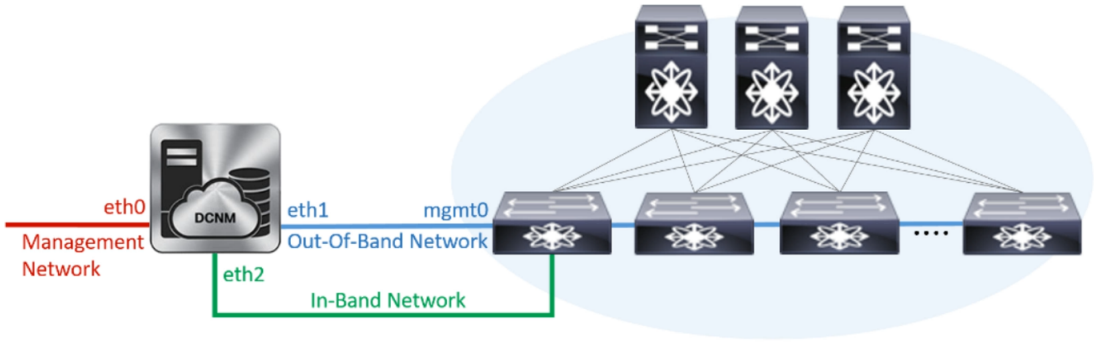
- **oobpool**: specifies the out-of-band pool; a smaller prefix of available IP addresses from the eth1 subnet. For example: Use 10.1.1.240/28 if the eth1 subnet was configured as 10.1.1.0/24 during installation.

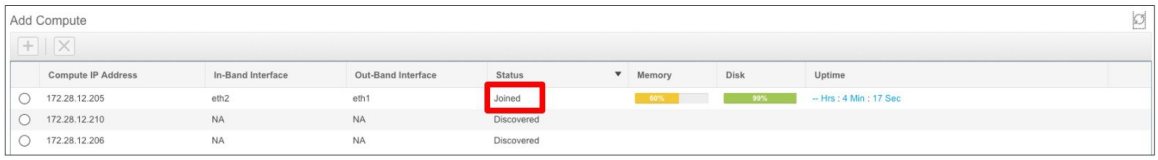
  This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

- **ibpool**: specifies the in-band pool; a smaller prefix of available IP addresses eth2 subnet. For example: Use 11.1.1.240/28 if the eth2 subnet was configured as 11.1.1.0/24 during installation.

  This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

- **computeip**: specifies the dcnm-mgmt network (eth0) interface IP address of the first compute node added to the cluster. This compute is added into the cluster as part of this command process and is used to migrate application data from DCNM servers to computes.





The other two computes are Discovered automatically, and is displayed on the Cisco DCNM **Web UI > Applications > Compute**.

The In-Band or out-of-band pools are used by services to connect with switches as required. The IP addresses from these pools must be available for configuration.

Note To add computes to the cluster mode, see Adding Computes into the Cluster Mode, on page 248.

Managing Application Network Pools

When you alter the eth1 or eth2 interface subnets, the corresponding oob pool and inband pool must be modified to match the new configuration. Network Insights and Endpoint Locator applications use the IP addresses from the Out-of-Band and In-Band pools.

To modify the IP addresses that are assigned to services running in the compute cluster, use the following command:

Note The inband or out-of-band pools are used by applications to connect with Cisco Nexus Switches. Hence, the IP addresses from these pools must be available and free.

appmgr afw config-pool [--ewpool *<InterApp-Subnet>]* **--oobpool** *<OutOfBand-Subnet>* **--ibpool** *<Inband-Subnet>***--compute***<compute-IP>*

Where:

- **ewpool**: specifies the east west pool subnet; for inter-service connectivity.

The network mask ranges from 20 to 24 These addresses aren't used directly between the computes, or to communicate with another node. These are used by containers to communicate with each other.

- **oobpool**: specifies the out-of-band pool; a smaller prefix of available IP Addresses from eth1 subnet.

  The network mask ranges from 24 to 28.

- **ibpool**: specifies the inband pool; a smaller prefix of available IP addresses from eth2 subnet.

  The network mask ranges from 24 to 28.

- **ipv6oobpool**: specifies the out-of-band IPv6 pool; a smaller prefix of available IPv6 addresses from eth1 subnet.

  If IPv6 is enabled, these addresses are required on both inband and out-of-band subnet.

  The network mask ranges from 112 to 124.

- **ipv6ibpool**: specifies the inband IPv6 pool; a smaller prefix of available IPv6 addresses from eth2 subnet.

  If IPv6 is enabled, these addresses are required on both inband and out-of-band subnet.

  The network mask ranges from 112 to 124.

Adding Computes into the Cluster Mode

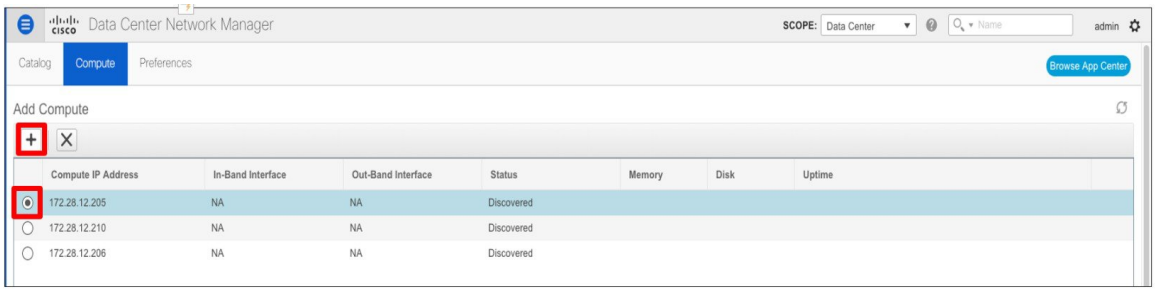
To add computes into the cluster mode from Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Applications** > **Compute**.

The Compute tab displays the computes enabled on the Cisco DCNM.

Step 2 Select a Compute node which is in **Discovered** status. Click the **Add Compute** (+) icon.



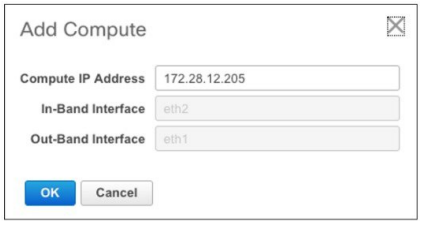
- While using Compute, ensure that Cisco DCNM GUI shows nodes as Joined.
- Offline indicates some connectivity issues, therefore no applications are running on Offline Computes.
- Failed indicates that the compute node could not join the cluster.
- Health indicates the amount of free memory and disk on the Compute node. The Health Monitor application provides more detailed statistics.
- Cisco DCNM 3 node cluster is resilient to single node failure only.

- If the Performance Manager was stopped during or after the inline upgrade and after all the computes have changed to Joined, you must restart the Performance Manager.

The Compute window allows you to monitor the health of computes. The health essentially indicates the amount of memory that is left in the compute, this is based on applications that are enabled. If a Compute is not properly communicating with the DCNM Server, the status of the Compute appears as Offline, and no applications are running on Offline Computes.

Step 3 In the **Add Compute** dialog box, view the **Compute IP Address**, **In-Band Interface**, and the **Out-Band Interface** values.

Note The interface value for each compute node is configured by using the **appmgr afw config-cluster** command.

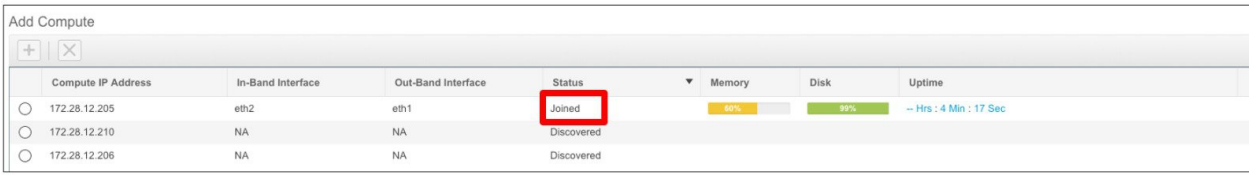


Step 4 Click **OK**.

The Status for that Compute IP changes to **Joining**.

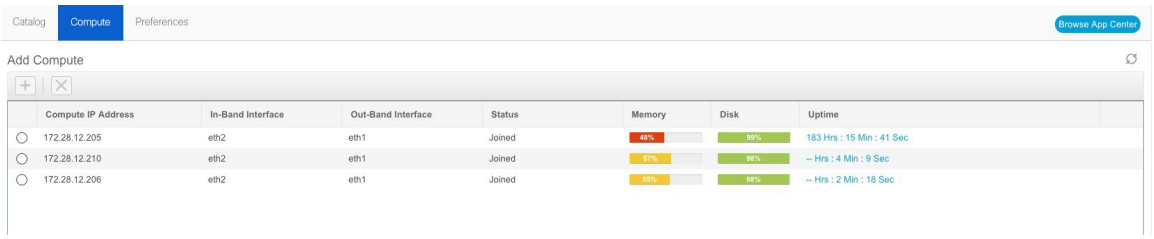


Wait until the Compute IP status shows **Joined**.



Step 5 Repeat the above steps to add the remaining compute node.

All the Computes appear as **Joined**.



Note When you install compute as a virtual machine on the VMware platform, vSwitch or DV switch port groups associated eth1 and eth2 must allow for packets that are associated with Mac address other than eth1 and eth2 to be forwarded.

Transitioning Compute Nodes

Transitioning Compute nodes from VM to Service Engine

To transition Cisco DCNM Compute Nodes from VMs to Applications Services Engine using the Cisco DCNM Web Client, perform the following steps:

Before you begin

- Ensure that Cisco DCNM Web Client is functioning.
- On the Cisco DCNM **Web Client > Applications > Compute**, all the Compute nodes must be in **Joined** state.

Procedure

Step 1 Choose **Applications > Compute**.

For example, let us indicate the three Compute nodes as **compute1** , **compute2** , and **compute3** .

Step 2 Open the vCenter Server application and connect to the vCenter Server with your vCenter user credentials.

Step 3 Navigate to **Home > Inventory > Hosts and Clusters** and identify the VM on which the DCNM Compute nodes are deployed.

Step 4 For **compute1**, make a note of the configurations and setup details provided during installation.

Step 5 Turn off **compute1**. Right click on the VM, select **Power off**.

On the **Web UI > Applications > Compute**, the status of **compute1** shows **Offline**.

Step 6 Using the configuration details of the compute node VM, install the compute node on Cisco Applications Services Engine.

For instructions, refer to *Installing DCNM Compute Node on Cisco ASE*.

Step 7 Launch the Web UI, and choose **Applications > Compute**.

The newly added compute automatically joins the cluster. The status of **compute1** changes from **Offline → Joining → Joined**.

Step 8 Repeat Steps Step 4, on page 250 to Step 7, on page 250 on **compute2** and **compute3** compute nodes.

After completion, all the Compute nodes on **Web UI > Applications > Compute** are in the **Joined** state.

All are Compute nodes are successfully hosted on the Cisco Applications Services Engine.

Transitioning Compute nodes from Service Engine to VM

To transition Cisco DCNM Compute Nodes from Applications Services Engine to VMs using the Cisco DCNM Web Client, perform the following steps:

Before you begin

- Ensure that Cisco DCNM Web Client is functioning.
- On the Cisco DCNM **Web Client > Applications > Compute**, all the Compute nodes must be in **Joined** state.

Procedure

Step 1 Choose **Applications > Compute**.

For example, let us indicate the three Compute nodes as **compute1** , **compute2** , and **compute3** .

Step 2 On the Cisco Applications Server console, for **compute1**, make a note of the configurations and setup details provided during installation.

Step 3 Power off the Applications Service Engine to turn off **compute1**.

On the Cisco DCNM **Web UI > Applications > Compute**, the status of **compute1** shows **Offline**.

Step 4 Using the configuration details of the compute node on Applications Service Engine, install the compute node on the VM.

Step 5 Launch the Web UI, and choose **Applications > Compute**.

The newly added compute automatically joins the cluster. The status of **compute1** changes from **Offline → Joining → Joined**.

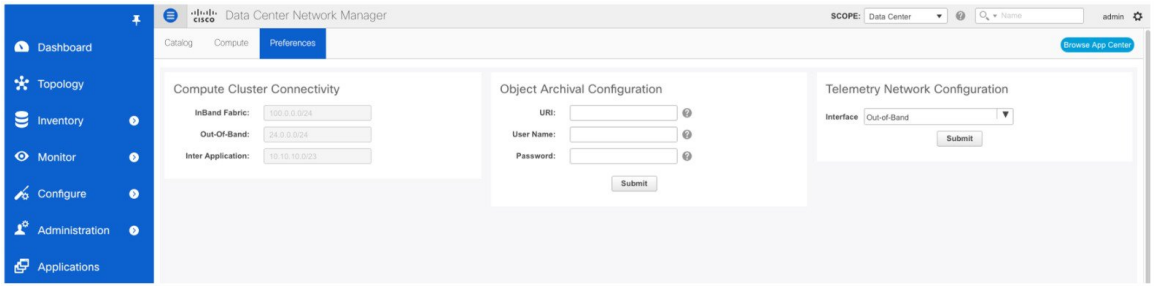
Step 6 Repeat Steps 3 to 5 on **compute2** and **compute3** compute nodes.

After completion, all the Compute nodes on **Web UI > Applications > Compute** are in the **Joined** state.

All are Compute nodes are successfully hosted on the VMs.

Preferences

This tab is relevant to the cluster mode of deployment, where the application instances are placed. This tab enables you to compute cluster connectivity and configure the Cluster Connectivity preferences.



Note This deployment does not support the compute cluster connectivity. The **Compute Cluster Connectivity** fields are grayed out for this deployment.

Object Archival Configuration

The NIA application collects tech support logs for all switches in Fabric, and determines the advisory, based on the data. The logs are saved on the Cisco DCNM server for further analysis or troubleshooting. If you need to download these logs before their life span ends or to create some space on the DCNM server, you can move the logs to a remote server.

In the **URI** field, enter the relative path to the archive folder, in the format `host[:port]/[path to archive]`. Enter the username and password to access the URI, in the **username** and **Password** field. Click **Submit** to configure the remote server.

Telemetry Network and NTP Requirements

For the Network Insights Resource (NIR) application, a UTR micro-services running inside the NIR receives the telemetry traffic from the switches either through Out-Of-Band (Eth1) or In-Band (Eth2) interface. By default, the telemetry is configured, and is streaming via the Out-Of-Band interface. You can choose to change it to In-Band interface as well.

Telemetry Using Out-of-band (OOB) Network

By default, the telemetry data is streamed through the management interface of the switches to the Cisco DCNM OOB network eth1 interface. This is a global configuration for all fabrics in Cisco DCNM LAN Fabric Deployment, or switch-groups in Cisco DCNM Classic LAN Deployment. After the telemetry is enabled via NIR application, the telemetry manager in Cisco DCNM will push the necessary NTP server configurations to the switches by using the DCNM OOB IP address as the NTP server IP address. The following example is sample output for **show run ntp** command.

```
switch# show run ntp

!Command: show running-config ntp
!Running configuration last done at: Thu Jun 27 18:03:07 2019
!Time: Thu Jun 27 20:32:18 2019

version 7.0(3)I7(6) Bios:version 07.65
ntp server 192.168.126.117 prefer use-vrf management
```

Installing and Deploying Applications

The following sections describes how to download, add, start, stop, and delete applications from the Cisco DCNM Web UI.

Download App from the App Store

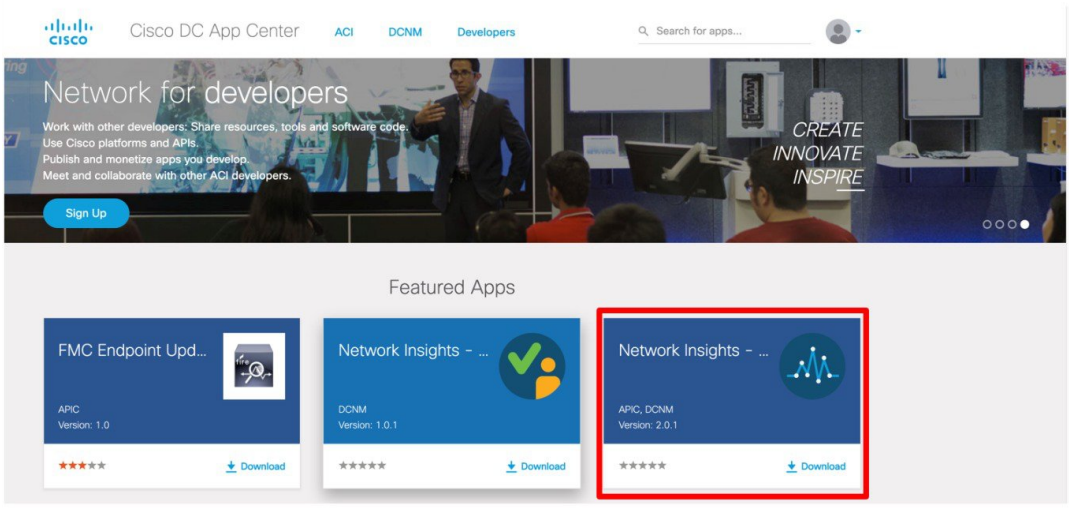
To download new applications from the Cisco DCNM Web UI, perform the following steps:

1. Choose **Applications**.

   By default, the **Catalog** tab displays.

2. Click **Browse App Center** on the top-right corner on the window.

   On the Cisco ACI App Center, locate the required application and click the download icon.



3. Save the application executable file on your local directory.

Add a New Application to DCNM

To add new applications from the Cisco DCNM Web UI, perform the following steps:

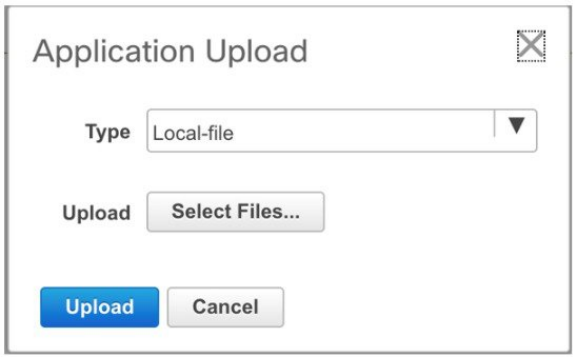
1. Choose **Applications**.

   By default, the **Catalog** tab displays.

2. Click **Add Application (+)** icon.



   On the Application Upload window, from the Type drop-down field, choose one of the following to upload the application.



From the Type drop-down list, select one of the following:

- If the file is located in a local directory, select **Local-file**.

  In the Upload field, click **Select files…**. Navigate to the directory where you have stored the application file.

  Select the application file and click **Open**.

  Click **Upload**.

- If the application is located on a remote server, select **Secure copy**.

Note Ensure that the remote server must be capable of serving Secure-copy (SCP).

In the URI field, provide the path to the application file. The path must be in `{host-ip}:{filepath}` format.

In the Username field, enter the username to access the URI.

In the Password field, enter the appropriate password for accessing the URI.

Click **Upload**.

After the application successfully uploaded, it is displayed in the Catalog window.

The green icon on the left-top corner indicates that the application is launched successfully and is operational. If there is no green icon on the application, it indicates that the application is not running. Click the application to Launch it.

Note Ensure that the Compute Cluster is enabled before you install applications. A few applications may not work is the compute cluster is configured after installing the applications.

Click the gear icon on the left-bottom on the application icon to view the Application Specifications. The Info tab displays the running container information. The Specs tab displays the configuration.

Starting Application

After the application is installed on the Cisco DCNM server, you must deploy the application. Click on the Application to begin deployment. Cisco DCNM starts all the services in the backend that are required for the application.

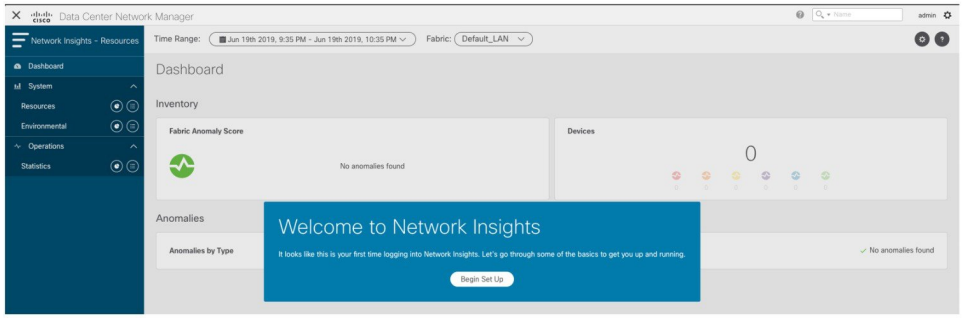


The green icon on the left-top corner indicates that the application is launched successfully and is operational.



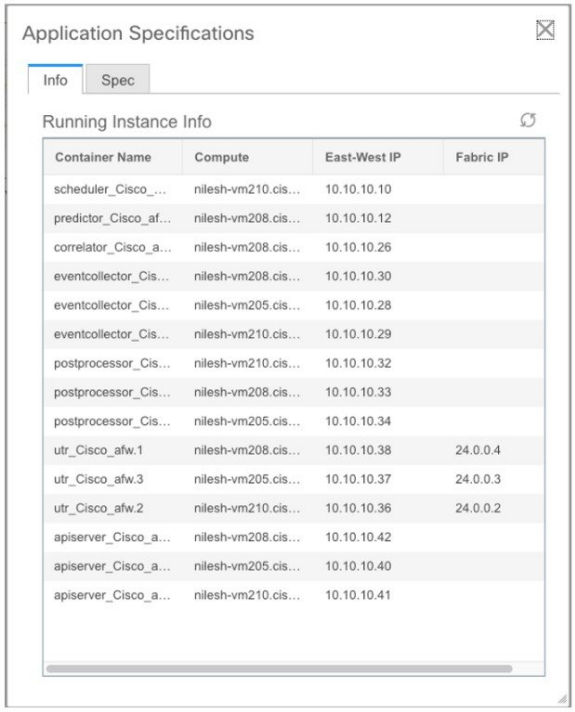
The applications utilizing the Kafka infrastructure services require three actively joined compute nodes, when you begin the application. For example, NIR and NIA applications. If the application has a user interface, after the application is successfully started the UI redirects to the index page served by the application.

If the application has a user interface, after the application is successfully started the UI redirects to the index page served by the application.



To check the services that are running go back to **Applications > Catalog**. Click the gear icon on the left-bottom on the application icon to view the Application Specifications. The Info tab displays the running container information and the Specs tab displays the configuration as shown in the figures below.





For information on how to remove computes from the cluster, stopping or deleting the applications, see Application Framework User Interface, on page 256.

Stop and Delete Applications

To delete the applications from the Catalog on the Cisco DCNM Web UI, perform the following steps:

1. Choose **Applications**.

   By default, the **Catalog** tab displays, showing all the installed applications.
2. Click the red icon on the right-bottom corner to stop the application.
3. Check the **Wipe Volumes** check box to erase all the data that is related to the application.
4. Click **Stop** to stop the application from streaming data from Cisco DCNM.

   The Green icon disappears after the application is successfully stopped.
5. After you stop the application, click the **Waste Basket** icon to remove the application from the Catalog.

Application Framework User Interface

To use the Applications Framework feature, in the Cisco DCNM home page's left pane, click **Applications**.

The Applications window displays the following tabs:

- **Catalog**—This tab lists the applications that are used by Cisco DCNM. These applications for performing various functions within Cisco DCNM. For more information, see *Catalog*.

- **Compute**—This tab displays the existing compute nodes. The tab shows nodes that are part of the hosting infrastructure. The uptime indicates how long they have been part of the infrastructure. In a High Availability (HA) setup, both the active and the standby nodes appear as joined. For more information, see Compute, on page 265.



Note In the cluster mode, the Cisco DCNM servers will not appear under the Compute tab.

- **Preferences**—This tab is relevant to the cluster mode of deployment, where the application instances are placed. This tab enables you to compute the cluster connectivity and configure the Cluster Connectivity preferences. For more information, see Preferences, on page 251.

Cisco DCNM uses the following applications:

- Compliance: This application helps in building fabrics for the Easy Fabric installation. The Compliance application runs as one instance per fabric. It is enabled when fabric is created. Similarly, it is disabled when fabric is deleted.
- Kibana: This is an open-source data-visualization plug-in for Elasticsearch, which provides visualization capabilities. Cisco DCNM uses the Kibana application for the Media Controller, and Endpoint Locator.
- vmmplugin: The Virtual Machine Manager (VMM) plug-in stores all the computes and the virtual machine information that connects to the fabric or the switch groups that are loaded into Cisco DCNM. VMM gathers compute repository information and displays the VMs, VSwitches/DVS, hosts in the topology view.
- Endpoint Locator: The Endpoint Locator (EPL) feature allows real-time tracking of endpoints within a data center. The tracking includes tracing the network life history of an endpoint and getting insights into the trends that are associated with endpoint additions, removals, moves, and so on. An endpoint is anything with an IP and MAC address. In that sense, an endpoint can be a virtual machine (VM), container, bare-metal server, service appliance and so on.

Catalog

The Catalog allows you to view all the applications that you have installed or enabled on the Cisco DCNM. Few applications are installed and are operational by default, when you install the Cisco DCNM.

The following applications appears based on the Cisco DCNM Deployments:

- Compliance (2.0)
- Debug plug-in (1.0)
- Kibana (1.1)
- Vmmplugin (3.0)
- Health Monitor (2.0)
- Endpoint Locator 2 (2.0)
- PTP Monitoring

Note The applications started by default, or also installed on the DCNM utilizes infrastructure services are operational, by default.

You can install more applications from the App Center, via the Web UI.

For instructions about downloading, adding, starting, stopping, and deleting applications from the Cisco DCNM Web UI, see Installing and Deploying Applications, on page 253.

Health Monitor

The Health Monitor helps you to monitor the infrastructure health and status. You can monitor the Alerts, Service Utilization, and Compute Utilization using the Health Monitor application. When you install or upgrade to 11.2(1), the Health Monitor application is installed and operational, by default.

To launch the Health Monitor app, on the Cisco DCNM Web UI, choose **Applications**. On the Catalog tab, click on **Health Monitor** to launch the application.

Note Health Monitor application is installed by default in Cisco DCNM cluster mode.

Health Monitor app broadly monitors and alerts on the following metrics for Services, Computes and DCNM server:

- CPU utilization
- Memory utilization
- Network I/O (eth0)
- Disk I/O

Note Health Monitor metrics can also be viewed in iReasoning or any other MIB browser/tool.

You can monitor the following using the Health Monitor application:

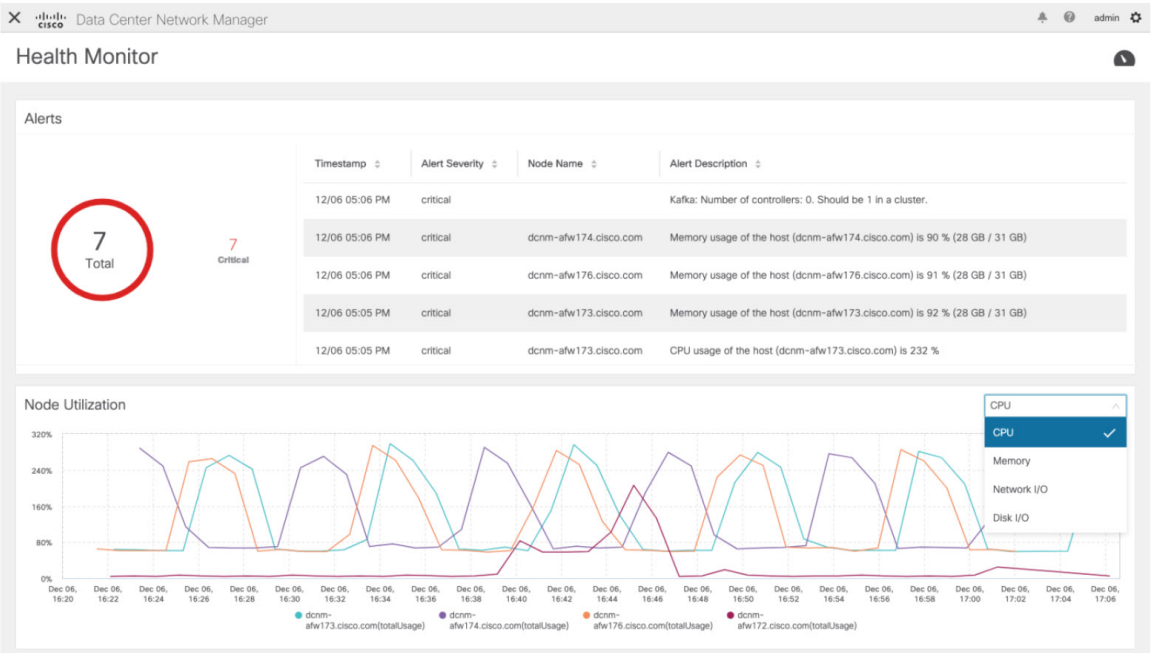
Alerts

The Alerts window provides information about the number of alerts that have occurred, from the specified date and time. You can view the alerts, based on the following categories, in the graphical view and the list view.

In the graphical view, the categories are:

- **Severity** displays the alerts, based on the severity: Critical/Major/Minor/Info.
- **Type** displays the alerts, based on the cluster type.
- **Compute** displays the alerts, for each compute node.
- **Service** displays the alerts, for all the services running on Cisco DCNM.

Click on the Refresh icon to refresh the alerts. Click on the list view icon to view the alerts in list format.



In the List View, alerts are displayed in tabular format with the following categories:

- **Timestamp** displays the time when the alert triggers. Format is MM/DD HH:MM AM/PM.
- **Alert Severity** displays the severity of alert.
- **Alert Type** displays the cluster alert type.
- **Node Name** displays the node name where the alert triggers.
- **Alert Description** displays the summary of the alert.

Click on the right or left navigation arrows to move to the next or the previous page.

You can also choose to set the number of items to view on page. Select a suitable number from the **Objects Per Page** drop-down list.

Click on the **Graphical representation** icon to go to the graphical view. Click on **Download Data** icon to download alerts information for troubleshooting purposes.

Health Monitor generates alerts for the following metrics:

- CPU utilization >= 65 %
- Memory utilization >= 65 %
- Disk utilization >= 65 %
- Elasticsearch cluster status: Red/yellow
- Elasticsearch unassigned shards > 0
- Elasticsearch JVM heap used >= 65 %
- Kafka partitions without leader: Controller offline partitions count > 0

- Kafka controllers count: Controller active controller count != 1
- Kafka partition leader: Controller unclear leader elections count > 0

Service Utilization

You can monitor all the services running on the Cisco DCNM on this window. Based on the time range and the service, the graphical view shows the CPU and Memory utilization for service. Click on the **Service Utilization** icon on the top-right corner to launch the CPU utilization graphical view.

From the **Time Range** drop-down list, choose the time range for which you want to view the utilization. You can select a specific time interval to view the metrics during that time interval. Click the fields showing the date and time to select the required date and time interval. You can also click the date on the calendar to set range. Click **Apply** to confirm the time range.

From the **Services** drop-down list, choose the service to view its Service utilization. This list comprises of all the services that are currently running on the Cisco DCNM.

Select the Time Range to view the **Service**, the **Cpu Utilization**, and **Memory Utilization** graphs. You can hover over specific points on the respective graphs for more information on CPU and Memory utilization at specific time.

The memory utilization graphical view depicts the actual memory consumption (RAM) in Gigabytes (GB).

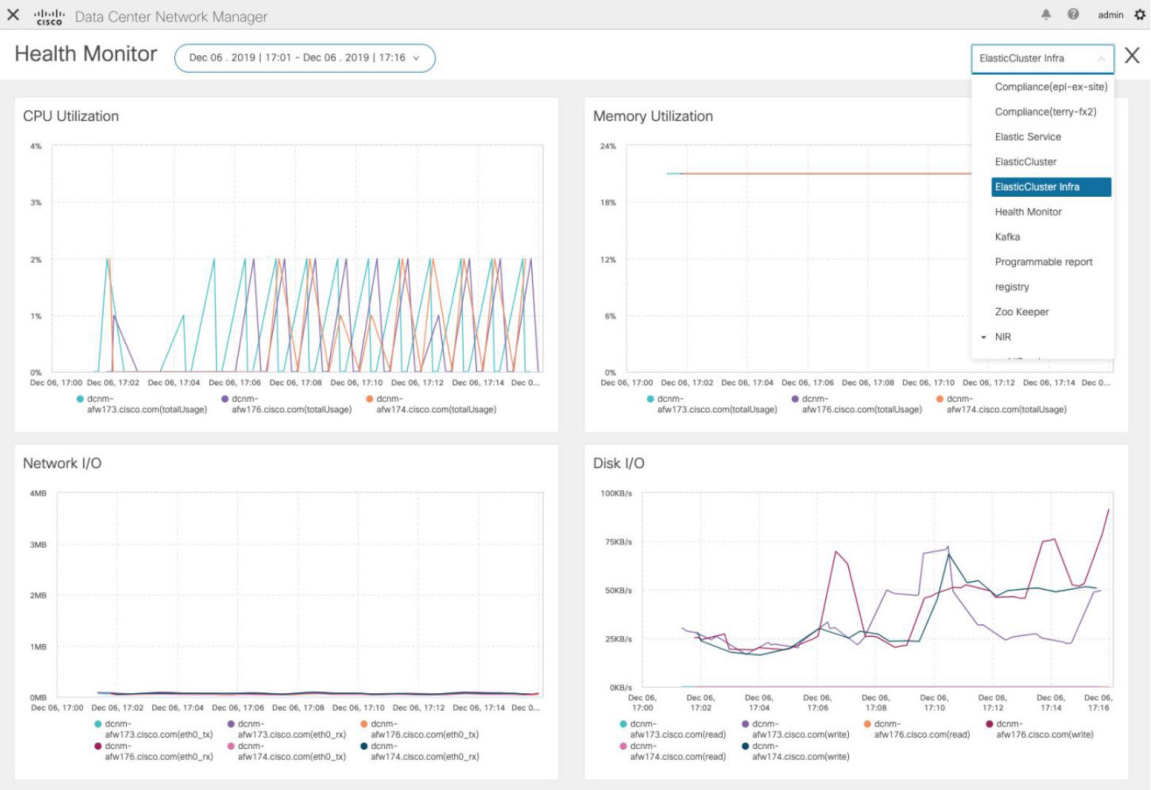
Click [**X**] icon on the top-right corner to close the Service Utilization window and revert to the Alerts window.

Guidelines and Limitations for Health Monitor in Service Utilization

- The CPU utilization for applications without a CPU limit, like Kafka, ElasticSearch, FMserver, and so on, may show 100% utilization in the graphs. 100% utilization is because this application uses one or more cores.
- The following alerts are triggered for the CPU utilization of applications:
  - Minor alert: 200-400 %

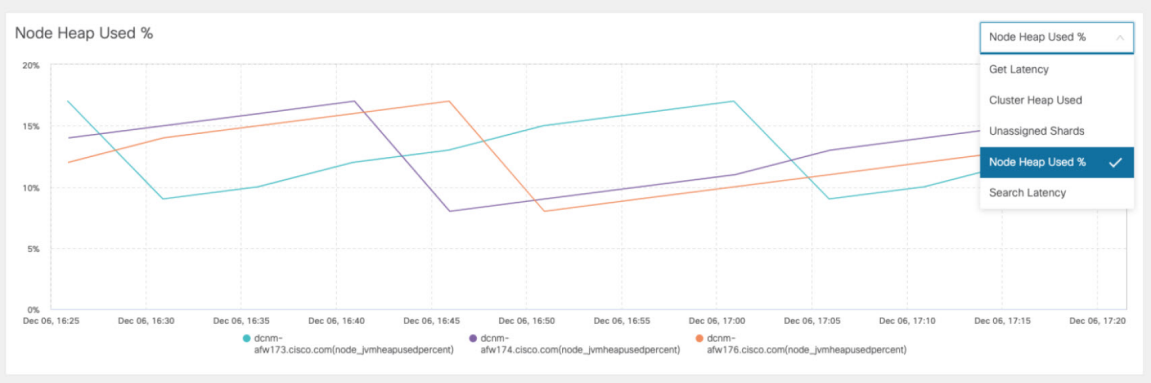
    Major alert: 400-600%

    Critical: > 600%
- The transient message for Kafka controller counts appears as a severe alert sometimes. You can ignore the alert if it clears within two minutes after refresh.
- The **Disk I/O** and **Memory Utilization** metrics are not available for Kafka and Elastic Service.
- The **Network I/O** metric is not available for **DCNM: FMServer** and **DCNM: Postgres**.
- The metrics does not auto-refresh. Navigate between different windows using the options in the drop-down list to refresh the metrics. Additionally, you can change the time range to refresh the metrics for a selected period.
- There might be duplicate alerts for the same feature.



The following additional metrics are collected for Elastic Cluster:

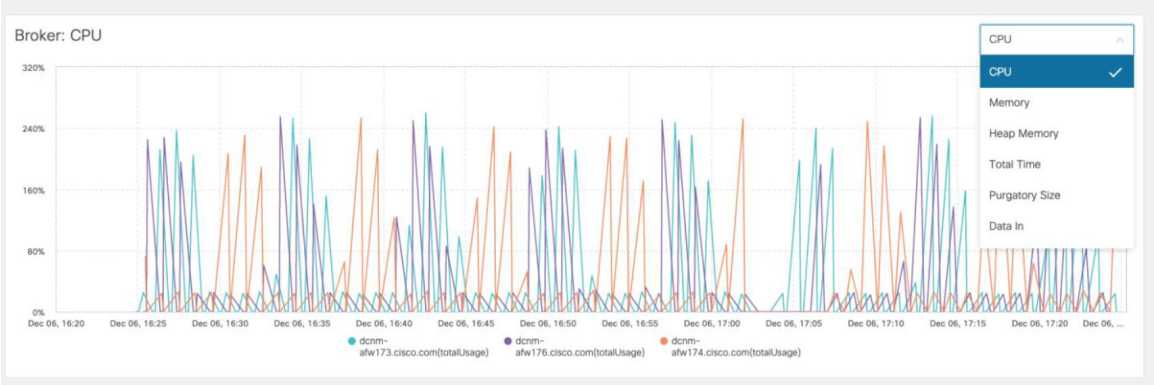
- Get latency: Latency for getting a single record by id
- Cluster heap used: Heap memory used by the cluster
- Unassigned shards: Count of unassigned shards
- Node heap used percentage: Percentage heap memory used by the node
- Search latency: Latency for getting a collection of records



The following additional metrics are collected for Kafka broker:

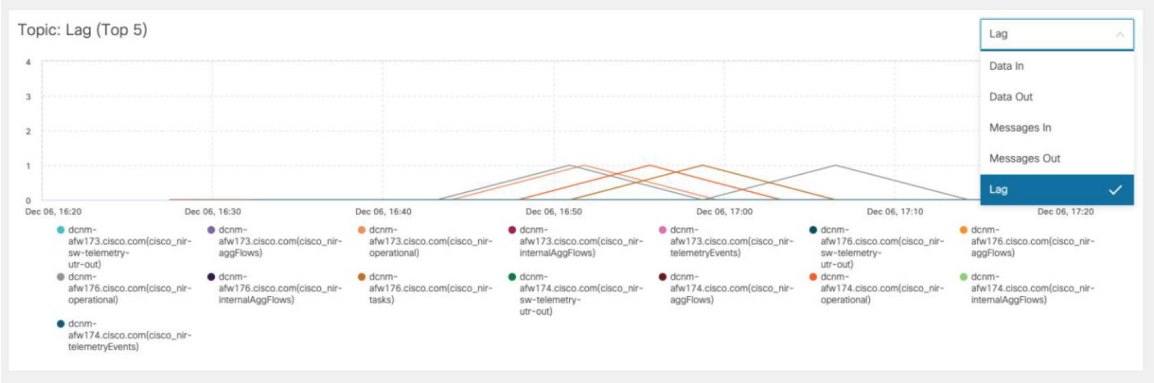
- CPU: CPU utilization of broker

- Memory: Memory utilization of broker
- Heap memory: Heap memory utilized by broker
- Total time: Network produce, network fetch follower, network fetch consumer time
- Purgatory size: Server fetch purgatory size, server produce purgatory size of broker
- Data in: Bytes in for the broker
- Data out: Bytes out for the broker
- Messages in: Messages received by the broker
- Fetch request: Total fetch requests for the broker
- ISR: In-sync-replicas expands and shrinks for the broker



The following additional metrics are collected for top 5 Kafka topics:

- Data in: Bytes in for the topic
- Data out: Bytes out for the topic
- Messages in: Message in count for topic
- Messages out: Message out count for topic
- Lag: Lag per topic



Compute Utilization

You can monitor all the computes installed with the Cisco DCNM. Based on the time range and the service, the graphical view shows the CPU and Memory utilization for service. Click on the **Compute Utilization** icon on the top-right corner to launch the CPU utilization graphical view.

From the **Time Range** drop-down list, choose the time range for which you want to view the utilization. You can select a specific time interval to view the metrics during that time interval. Click the fields showing the date and time to select the required date and time interval. You can also click the date on the calendar to set range. Click **Apply** to confirm the time range.

Select the Time Range to view the **Service**, the **Cpu Utilization**, and **Memory Utilization** graphs. You can hover over specific points on the respective graphs for more information on CPU and Memory utilization at specific time.

The memory utilization graphical view depicts the actual memory consumption (RAM) in Gigabytes (GB).

Click [**X**] icon on the top-right corner to close the Service Utilization window and revert to the Alerts window.

PTP Monitoring

This section explains the functionality of the Precision Time Protocol (PTP) monitoring. PTP is a time synchronization protocol for nodes that are distributed across a network. On a local area network, it achieves clock accuracy in the sub-nanosecond range, making it suitable for measurement and control systems.

In DCNM, PTP Monitoring can be installed as an application. From the DCNM Web UI, navigate to **Applications** and click **PTP Monitoring**. This application works in the IPFM mode only.

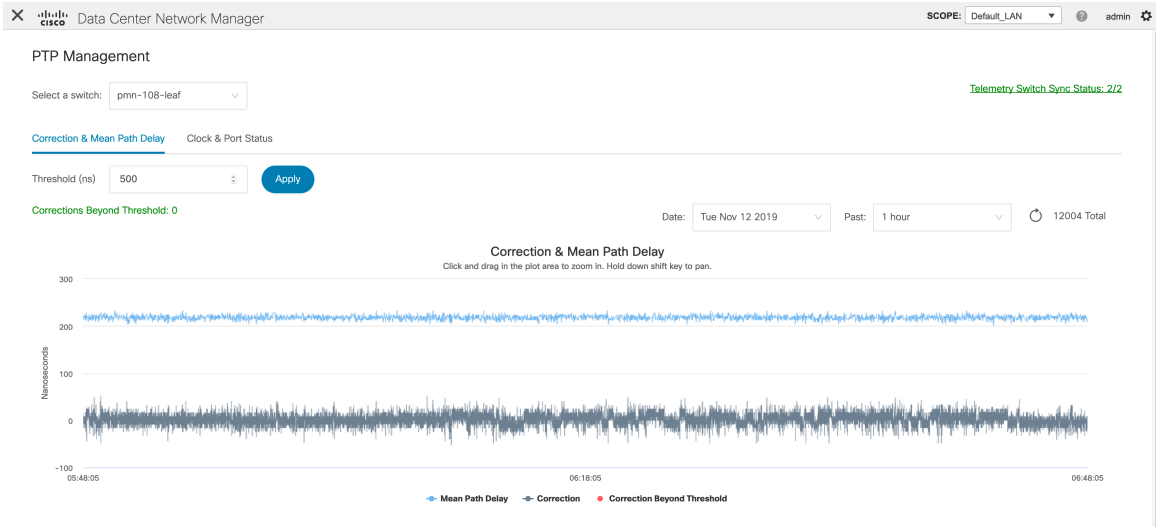
In the **PTP Management** window, you can view PTP related information based on the switch selected from the **Select a switch** drop-down list. You can click the **Telemetry Switch Sync Status** link to check whether the switches are in sync. The **Sync Status** column displays the status of the switches.

The following tabs are displayed in this window:

- **Correction & Mean Path Delay**
- **Clock & Port Status**



Note The PTP related info is displayed for the switch group that you select from the **SCOPE** drop-down list.



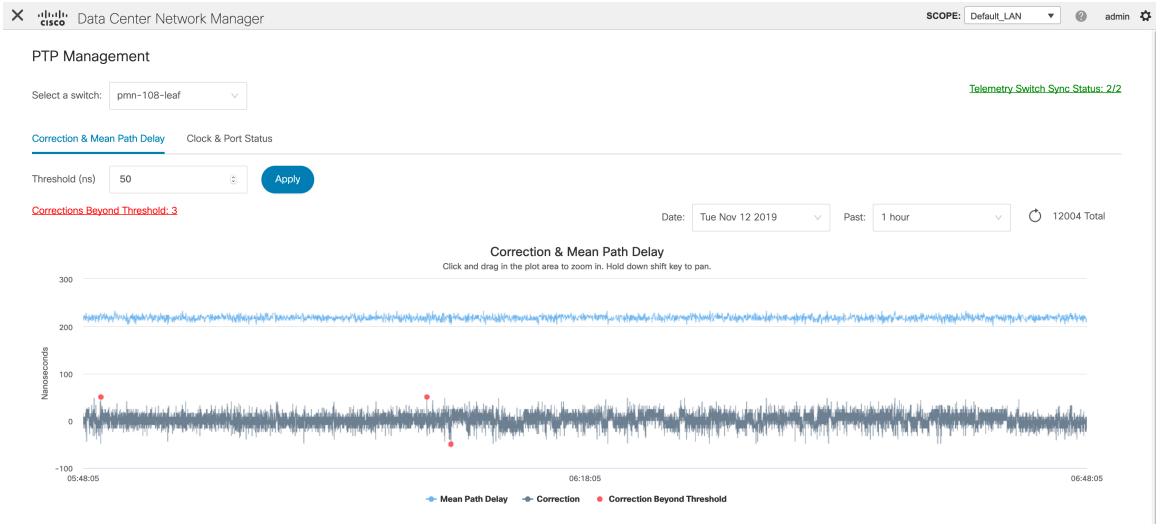
Correction and Mean Path Delay

The **Correction & Mean Path Delay** tab displays a graph showing the PTP operational statistics: mean path delay, correction, and correction beyond threshold. You can click and drag in the plot area to zoom in and hold the **shift** key to pan. Click the **Reset zoom** button to reset zoom.

By default, the graph is displayed for the threshold value of 500 nanoseconds (ns). You can also display data based on a specific threshold value. In the **Threshold (ns)** field, enter the required value in nanoseconds and click **Apply**. Note that the threshold value is persistent in the DCNM settings, and it is used to generate PTP correction threshold AMQP notifications.

From the **Date** drop-down list, you can select the appropriate date to view the data. The PTP data is stored up to the last seven (7) days. The default value for the stored data is 7 days. To change this value, navigate to **Administration > DCNM Server > Server Properties** and set the updated value for the **pmn.elasticsearch.history.days** property.

From the **Past** drop-down list, you can also select a timeframe over which the data has to be displayed. The values in the **Past** drop-down list are 1, 6, 12, and 24 hours.



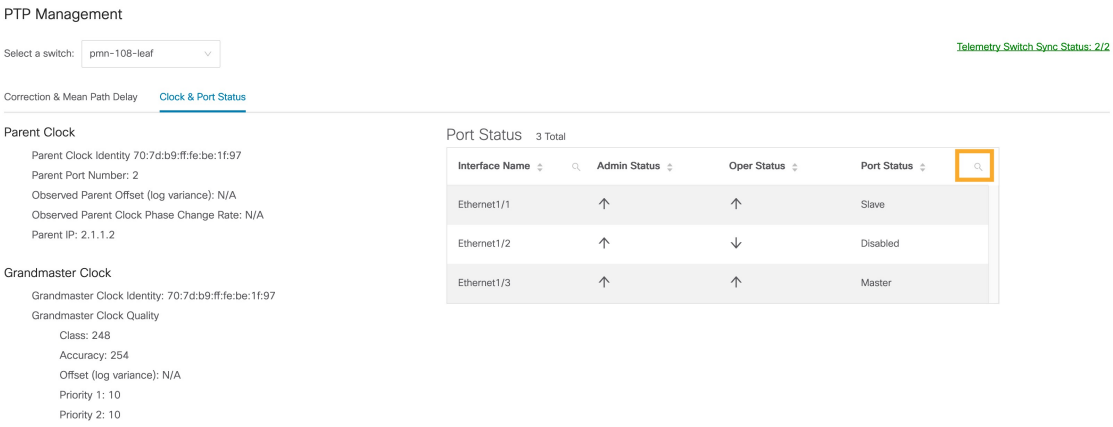
Note that you can click the legends in the graph to hide or display statistics.

If there are any corrections, you can view them in a tabular format by clicking the **Corrections Beyond Threshold** link.



Clock and Port Status

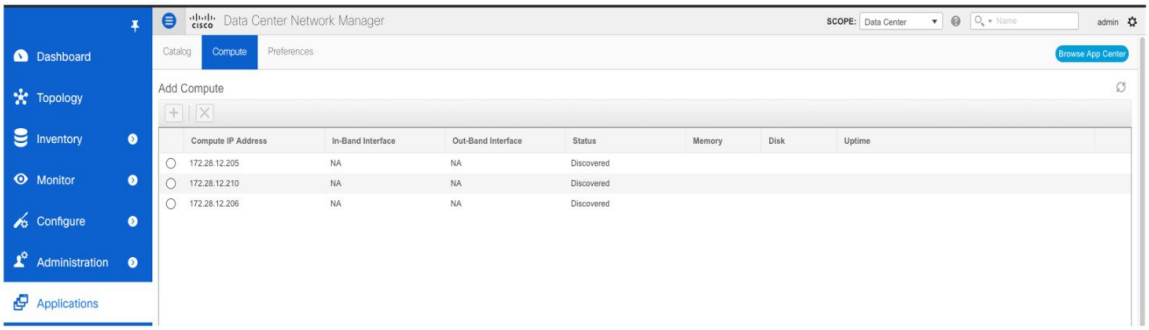
The **Clock & Port Status** tab displays status for Parent Clock, Grandmaster Clock, and ports.



The **Port Status** table displays the status of the ports. Click the **Search** icon, and enter the port status, and click **Search** to filter the port status.

Compute

This tab displays the existing compute nodes. The tab shows nodes that are part of the hosting infrastructure. The uptime indicates how long they have been part of the infrastructure. In a High Availability (HA) setup, both the active and the standby nodes appear as joined. In clustered mode, the compute nodes status indicate if the nodes are joined or discovered.



Note If the NTP server for compute nodes is not synchronized with the NTP server for DCNM Servers (Active and Standby) and Computes, you cannot configure a cluster.

The certificates are generated with a timestamp. If you configure the Compute nodes using a different NTP server, the mismatch in timestamp will not allow to validate the certificates. Therefore, if the compute cluster is configured despite of a mismatch of NTP server, the applications will not function properly.

Note In clustered mode, the Cisco DCNM servers will not appear under the Compute tab.

The following table describes the fields that appear on **Applications > Compute**.

Table 48: Field and Description on Compute Tab

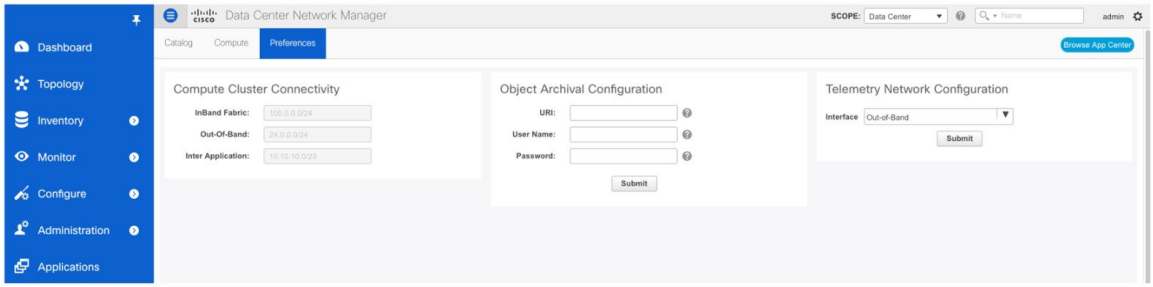
Field	Description
Compute IP Address	Specifies the IP Address of the Compute node.
In-Band Interface	Specifies the in-band management interface.
Out-Band Interface	Specifies the out-band management interface.
Status	Specifies the status of the Compute node. • Joined • Discovered • Failed • Offline
Memory	Specifies the memory that is consumed by the node.
Disk	Specifies the disk space that is consumed on the compute node.
Uptime	Specifies the duration of the uptime for a compute node.

When you install a compute node with correct parameters, it appears as **Joined** in the Status column. However, the other two computes appears as Discovered. To add computes to the cluster mode from Cisco DCNM Web UI, see Adding Computes into the Cluster Mode, on page 248.

To configure or modify the Cluster Connectivity preferences, see Preferences, on page 251.

Preferences

This tab is relevant to the cluster mode of deployment, where the application instances are placed. This tab enables you to compute cluster connectivity and configure the Cluster Connectivity preferences.



Note This deployment does not support the compute cluster connectivity. The **Compute Cluster Connectivity** fields are grayed out for this deployment.

Object Archival Configuration

The NIA application collects tech support logs for all switches in Fabric, and determines the advisory, based on the data. The logs are saved on the Cisco DCNM server for further analysis or troubleshooting. If you need to download these logs before their life span ends or to create some space on the DCNM server, you can move the logs to a remote server.

In the **URI** field, enter the relative path to the archive folder, in the format `host[:port]/[path to archive]`. Enter the username and password to access the URI, in the **username** and **Password** field. Click **Submit** to configure the remote server.

Failure Scenario

Recommendation for minimum redundancy configuration with a DCNM OVA install is as follows:

- DCNM Active Node(Active) and compute node 1 in server1.
- DCNM Standby Node and compute node 2 in server2.
- Compute node 3 in server3.

When DCNM Active node is down, the Standby node takes full responsibility of running the core functionality.

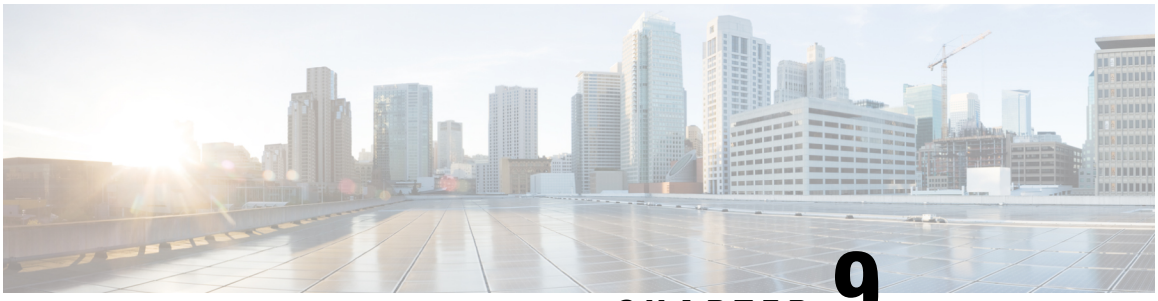
When a compute node is down, the applications may continue to function with limited functionality. If this situation persists for a longer duration, it affects the performance and reliability of the applications. When

more than one node is down, it affects the applications functionality and most of the applications fail to function.

You must maintain 3 compute nodes at any time. If a compute node goes down, rectify the issue as soon as possible, for the services to function as expected.

Compute Node Disaster Recovery

When a compute node is lost due to a disaster and is irrecoverable, you must install another compute node with the same parameters. This will essentially appear as a reboot of the compute with lost data and it tries to join the cluster automatically. After it joins the cluster, all the data will synchronize from the other two compute nodes.



CHAPTER 9

DCNM Integration with ServiceNow

• DCNM Integration with ServiceNow, on page 269

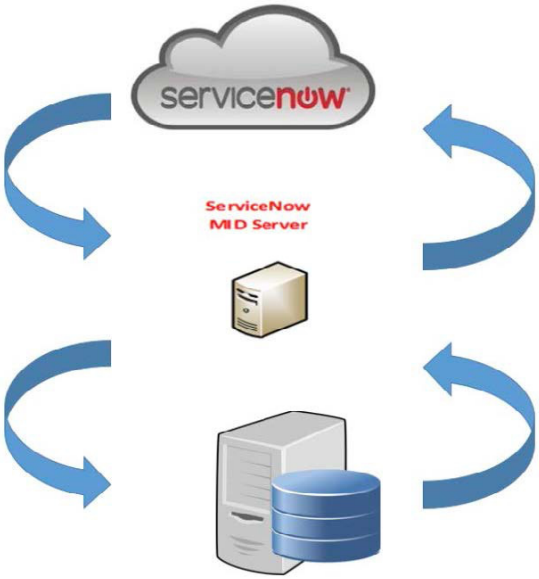
DCNM Integration with ServiceNow

ServiceNow offers applications for IT Service Management (ITSM) and IT Operations Management (ITOM). There are four primary modules - inventory discovery, incident management, event management & change management workflows. Starting from Cisco DCNM Release 11.3(1), we provide Cisco DCNM integration with ServiceNow. This enables you to integrate end-user IT data with the ServiceNow platform. The integration provides a default set of ServiceNow custom tables which are populated with configuration data.

To utilize this functionality, install the DCNM application in the ServiceNow customer instance and provide the DCNM mid-server details. Information or data regarding switch details, port details, and alarms, is retrieved to the ServiceNow Configuration Management Database (CMDB) tables. By default, data is retrieved every 15 minutes and displayed.

Details about the switches and ports of each switch are collected from the DCNM inventory. The alarms are collected by polling DCNM. Alarms are then filtered and categorized based on their type, such as, CPU, MEMORY, POWER, LINKSTATE, EXTERNAL, ICMP, SNMP, and SSH. The alarms are then stored in an Events table. These events are then used to generate incidents for the CPU, MEMORY, SNMP, and SSH categories. The source, description, severity and category of each alarm is stored. When an alarm is cleared on DCNM, it is also cleared on ServiceNow in the next poll cycle. When polling of alarms is initiated for the first time, the alarms that were raised in the last seven days are pulled in from DCNM. In case there is a gap of more than seven days between collection of alarms, the old alarms are cleared and the polling process is reinitiated.

The DCNM application on ServiceNow runs scheduled scripts and connects with the mid-server which in turn connects with DCNM to retrieve data. The DCNM sends the requested data to the mid-server which then passes on the data to DCNM application on ServiceNow. The tables in the DCNM instance on ServiceNow are then populated with this retrieved data.



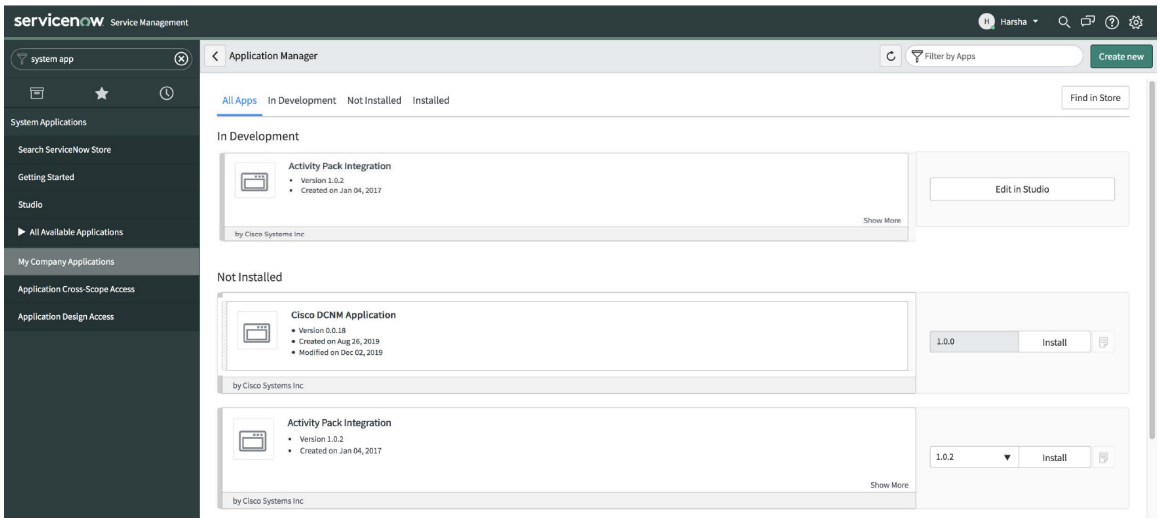
Guidelines and Limitations of DCNM Integration with ServiceNow

- Details about only one mid-server should be added in the **Cisco DCNM>Properties** table.
- Scheduled scripts to retrieve data are run only after insertion of a server record in the **Cisco DCNM>Properties** table.
- In case the mid-server IP Address and credentials in the **Cisco DCNM>Properties** table are changed, the data that was imported using the previous mid-server is deleted from the application scope tables. However, data that was imported to the ServiceNow CMDB (global scope) remains and is not deleted.
- To ensure optimal performance in the ServiceNow database, each entry is matched with the switch database ID and IP Address ensuring that there is no duplication of entries.
- Entries in the cmdb_ci_ip_switch table have to be manually deleted in case a new server is added in the **Cisco DCNM>Properties** table.

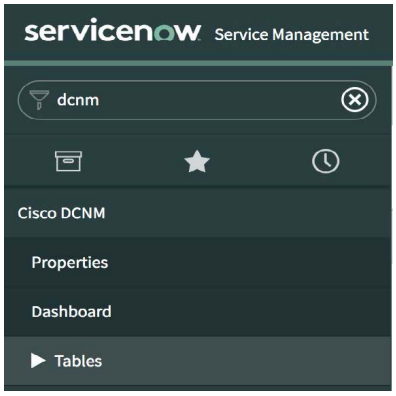
Installing and Configuring the Cisco DCNM Application on ServiceNow

Procedure

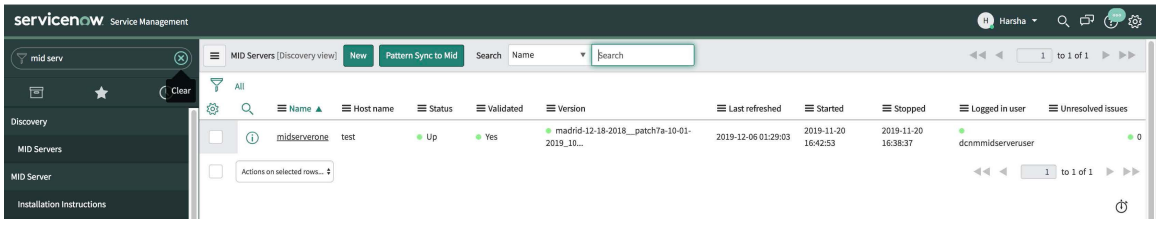
Step 1 Log in to https://dcnm1.service-now.com. Select **System Applications** > **Applications**. Install the **Cisco DCNM Application** from the **All Apps** tab.



Step 2 After installation is complete, verify that the Cisco DCNM Properties and Dashboard tabs are appearing in the application.

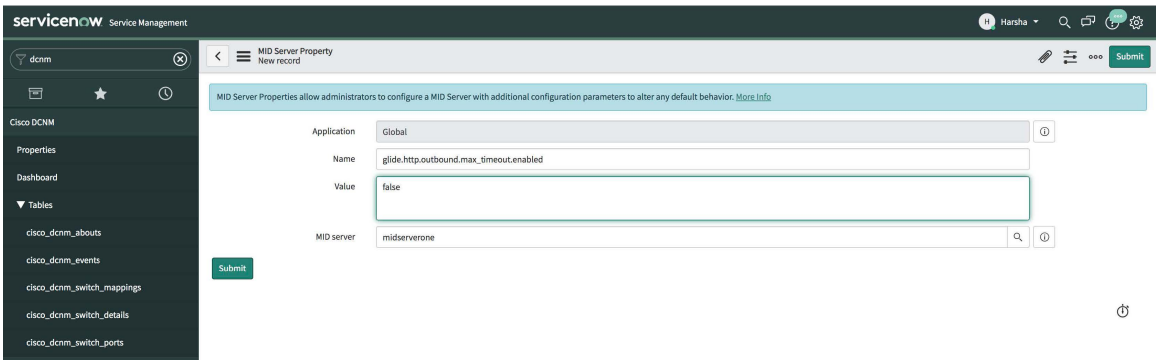


Step 3 Choose **MID Servers** and click the MID Server that is used for DCNM integration.

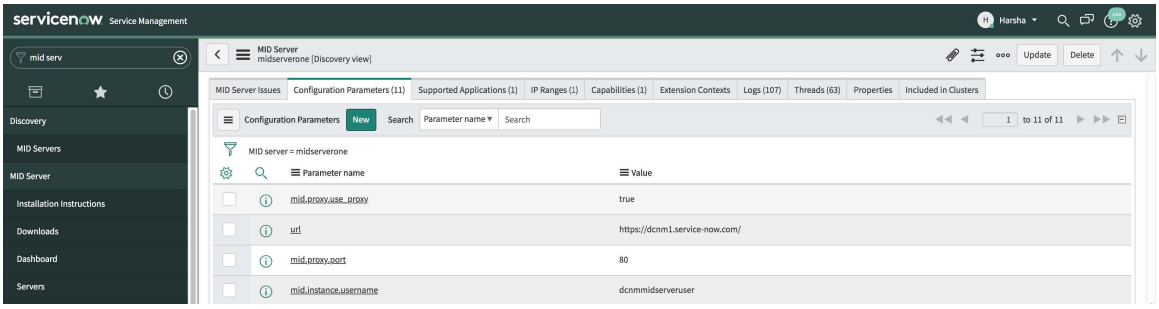


Step 4 Scroll down and click the **Properties** tab. Click **New** and add the property given below in the **MID Server Property New record** window. Click **Submit**.

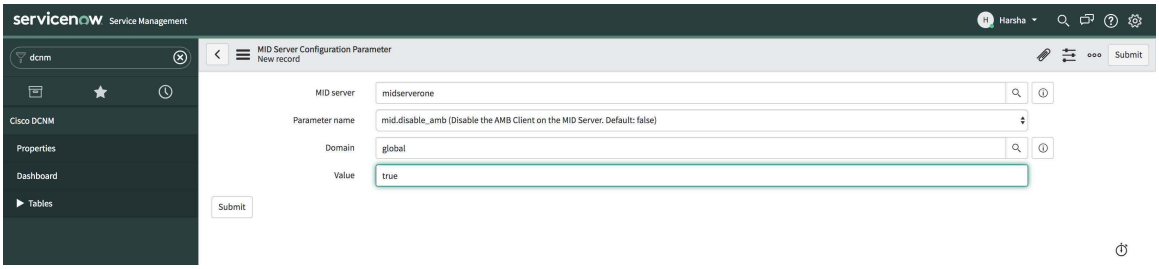
Name	Type	Value
glide.http.outbound.max_timeout.enabled	True/false	False



Step 5 Now, select the **Configuration Parameters** tab.

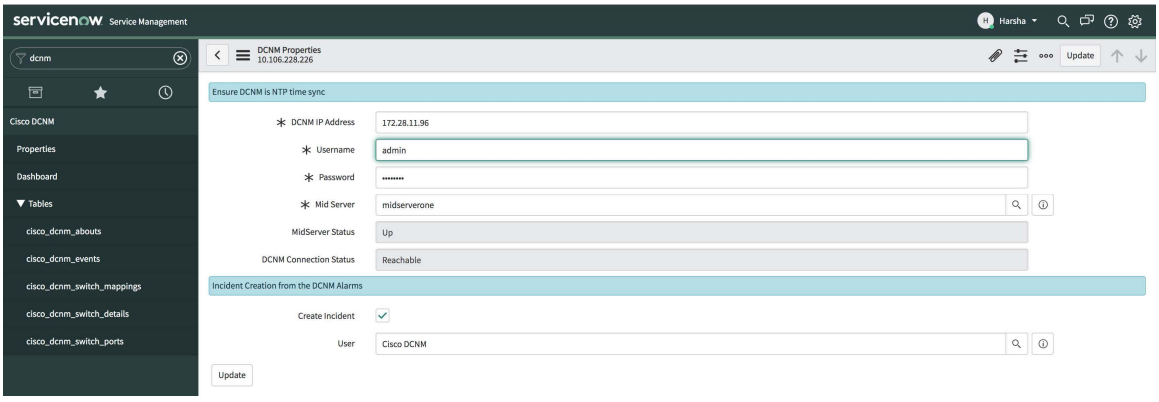


Step 6 In the **Configuration Parameters** tab, click **New**. Enter the required details in the fields.



Step 7 Click **Submit** to set up the MID Server.

Step 8 Choose **Cisco DCNM > Properties**. Click **New Server**. Enter the required parameters.



DCNM IP Address - IP Address of the DCNM.

Username - Enter the username used to log in to DCNM.

Password - Enter the password used to log in to DCNM.

Note Access should be provided only for DCNM admins.

Mid server - Specify the name of the midserver to be used. The name is auto-populated as you type. You can also click the search icon next to this field to bring the MID Servers window. You can then select a MID Server from the list that is displayed.

User - Create a new user and add the user name in this field. The Caller field in the incidents that are created is populated with this user name. This field is auto-populated as you type. You can also click the search icon next to this field to bring the Users window. You can then select a user from the list that is displayed.

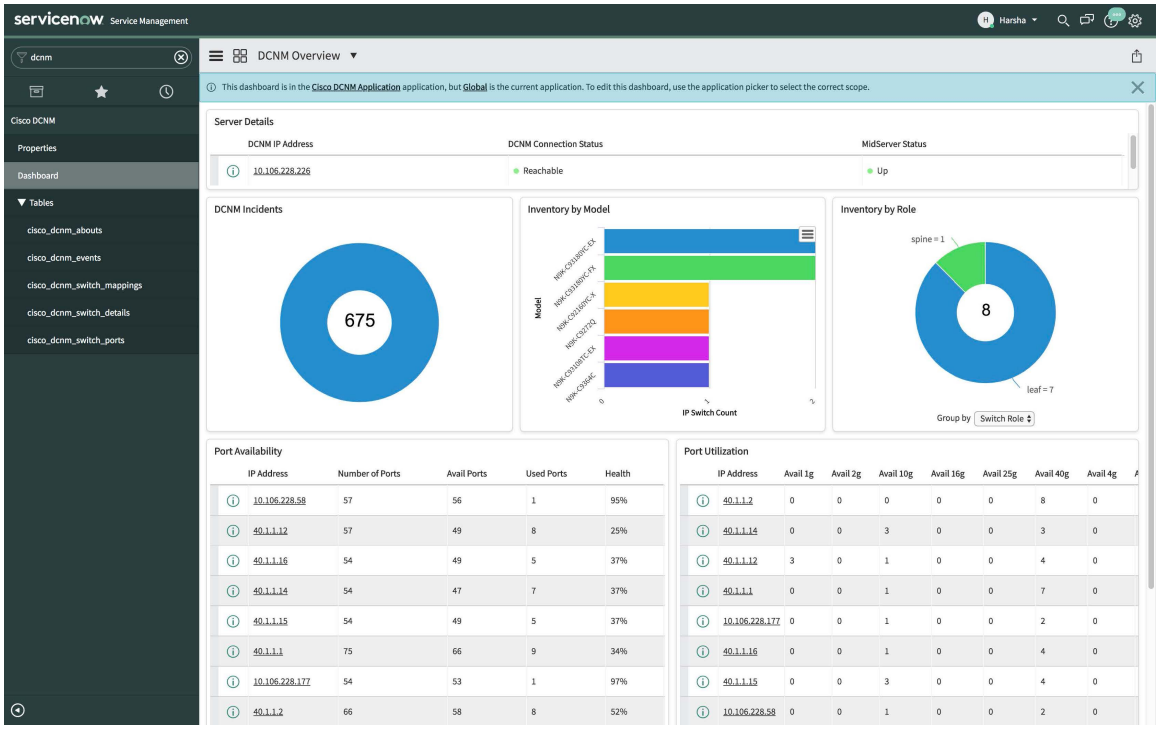
Create Incident - Select this checkbox in case you need incidents to be raised automatically for alarm events.

Now, Click **Submit**.

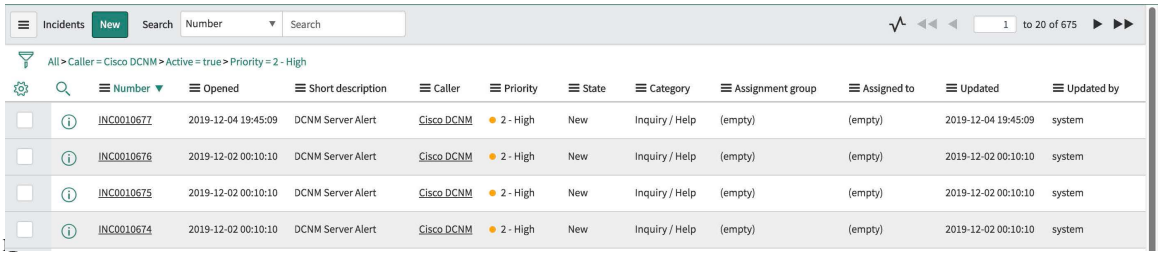
After the server details are submitted, the **DCNM Connection Status** field will display **Reachable** on successful communication with DCNM, and **Unreachable**, in case the connection is unsuccessful.

Viewing the Dashboard

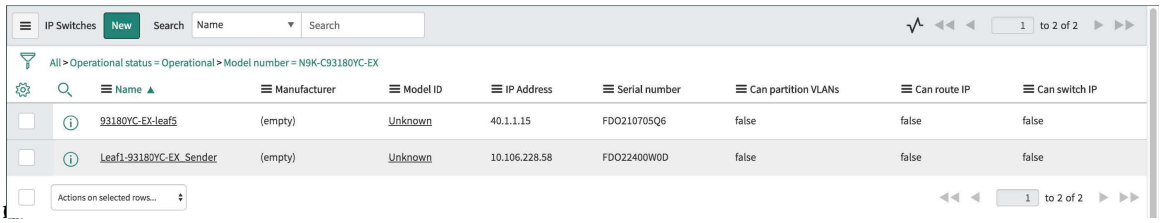
Choose **Cisco DCNM>Dashboard** to display the dashboard. The **DCNM IP Address**, the **DCNM Connection Status** and the **MidServer Status** are displayed at the top of the dashboard.



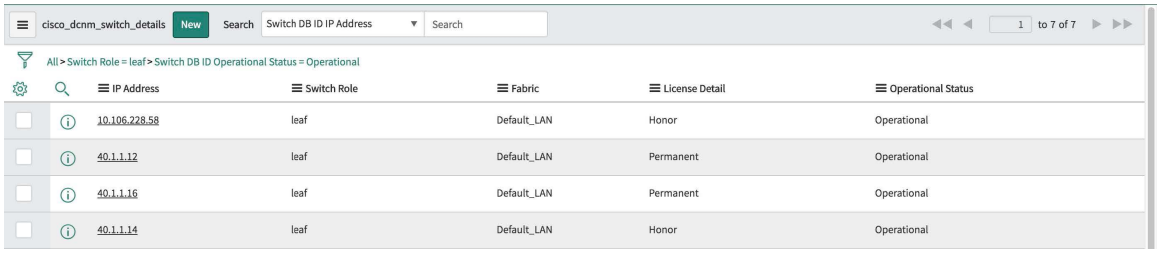
DCNM Incidents - This displays the number of incidents that have been raised based on the alarms retrieved from DCNM. Click the donut for more details about the



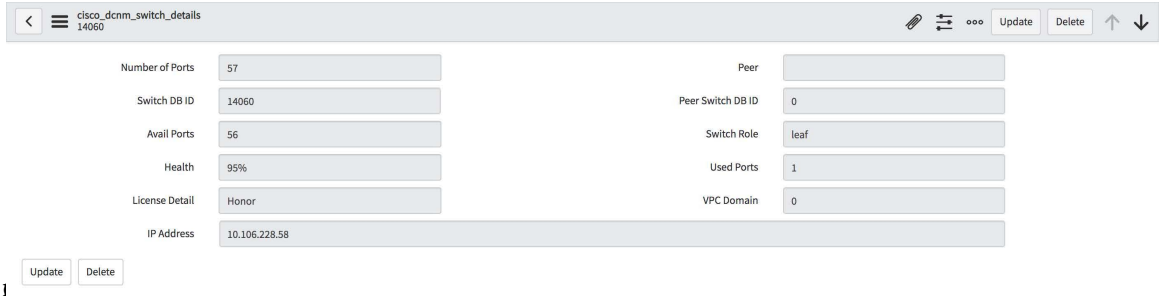
Inventory by Model - This displays the number and type of switches present in DCNM. Each band represents a device model. Click a band for more



Inventory by Role - This displays the number and types of switch roles present in DCNM. Click the required section to display the number of roles that are operational and click on that pictorial representation to display more details about the

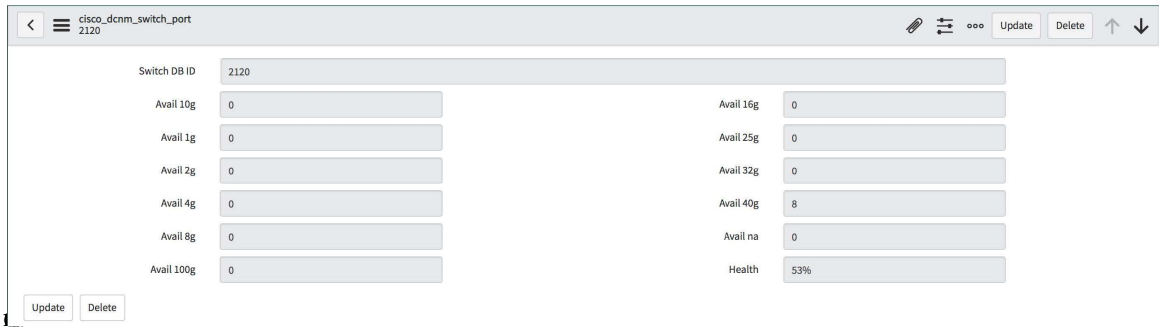


Port Availability - This displays information about port availability. The IP address along with the total number of ports, available ports, used ports and health of the switch id displayed. Click an IP address to display more



Port Utilization - This displays information about port utilization based on each IP address. The number of ports having 1G, 2G, 4G, 8G, 10G, 16G, 25G, 32G, 40G, and 100G availability, are displayed. Click an IP

address to display more



Troubleshooting DCNM Integration with ServiceNow

In case data is not being retrieved in the ServiceNow table:

- Check if the MID server is up or down.
- Check for information entries in system logs with the source “x_caci_cisco_dcnm”.
- Check the login credentials added in Cisco DCNM Properties.

For more information on DCNM application integration with ServiceNow, click here.