Configure

This section contains context-sensitive Online Help content for the **Web Client > Configure** tab.

Deploy

The Deploy menu includes the following submenus:

Configuring vPC Peer

A virtual PortChannel (vPC) allows links that are physically connected to two different Cisco Nexus devices to appear as a single PortChannel to a third device. The third device can be a Cisco Nexus 2000 Series Fabric Extender or a switch, server, or any other networking device. A vPC can provide Layer 2 multipathing, which allows you to create redundancy by increasing bandwidth, enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.

After you enable the vPC function, you create a peer keepalive link, which sends heartbeat messages between the two vPC peer devices.

The vPC domain includes both vPC peer devices, the vPC peer keepalive link, the vPC peer link, and all the PortChannels in the vPC domain connected to the downstream device. You can have only one vPC domain ID on each device.

vPC creation is divided into two steps, vPC Peer creation and vPC creation. To configure vPC user first needs to configure vPC domain. To create vPC Peer, navigate to **Configure > Deploy > vPC Peer**.

Note After you configure the vPC peer, select vPC peer using the radio button and click **Add vPC**. For information about how to add a vPC to the selected vPC peer, see Add vPC, on page 7.

You can view the history of tasks performed, navigate to **Configure > Deploy > vPC Peer > History** tab. For more information, see vPC Peer History, on page 2.

You can view the list of vPC domains in the **Pre Configured Peers** table.

Table 1: Pre Configured Peers

Column	Description
Search box	Enter any string to filter the entries in their respective column.
Domain ID	Displays the domain ID of the vPC peer switches.
Primary Switch	Displays the vPC Primary device name.
Primary Port Channel ID	Displays the peer-link port channel for vPC primary device.
Secondary Switch	Displays the vPC secondary device name.
Secondary Port Channel ID	Displays the peer-link port channel for vPC secondary device.
Consistency	Displays the vPC Consistency status. Corresponds vPC peer-link configuration and Global Consistency parameters.

This feature supports add, delete, and edit option for Domain. You can also view vPC Peer History.

vPC Peer History

To view the deployed jobs on the vPC peers, navigate to **Configure > Deploy > vPC Peer > History** tab. You can view the list **vPC Peer History** information in the Table 2: vPC Peer History, on page 2.

Table 2: vPC Peer History

Column	Description
Domain Id	Specifies the domain ID for the vPC peer
Primary Switch	Specifies the Primary Switch associated with the vPC Peer.
Secondary Switch	Specifies the Secondary Switch associated with the vPC Peer.
Created By	Specifies the DCNM username, who deployed this task.
Started At	Specifies the time at which the task was performed on the vPC peer. The time is displayed in the format YYYY-MM-DD HH:MM:SS.
Task Performed	Specifies the task that is performed on the vPC peer.

Column	Description
Status	Species the status of the task that is performed on the vPC Peer. The status can be Failed, Success, or in_progress.
View Command History	Select an activity, click **View Command History**. The Command History page displays the commands that are executed, status, and error message on the **Primary Switch** and **Secondary Switch**, in their respective tabs.
Delete vPC Peer Job	Select a vPC Peer History entry and click **Delete** to delete the task history.

Add vPC Peer Wizard

You can launch the vPC Peer configuration wizard by clicking the **Add vPC Peer** icon in the toolbar.

Procedure

Step 1 From the menu bar, choose **Configure > Deploy > vPC Peer** tab.

Step 2 Click the **Add vPC Peer** icon in the toolbar.

You are directed to the vPC Peer creation wizard. There are five steps to complete the vPC Peer creation.

Step 3 On the Select Devices screen:

Click to choose the device that you want to be the primary and device secondary device on the vPC peer link. You can also filter the devices using the **Scope** drop-down list.

Note The licensed devices with configured LAN credentials are displayed.

Note If vPC is already configured on the device that you chose as primary, the secondary device information and the domain ID are populated automatically. You can also modify, as required.

In the **Domain ID** field, enter the vPC domain ID.

To enable LACP on peer link, check the **Enable lacp on peer link** checkbox.

For VXLAN VTEP device, **Loopback Interface** and **Loopback Secondary IP** address can be specified in the Domain Setting table.

Click **Next** to configure peer link.

Step 4 On the Configure Peer-Link screen:

For configuring the peer-link, you have two options. You can either select an existing port-channel or create a new port-channel. If Peer link is already configured on device, on selection of peer link port-channel automatically populates secondary peer-link port-channel.

Perform the following steps on both the primary and the secondary devices.

1. Click **Existing Port Channel** or **Create New port Channel** radio button to configure port channel.

A port channel bundles physical links into a channel group to create a single logical link that provides the aggregate bandwidth of up to 8 physical links on the M series module. If a member port within a port channel fails, the traffic previously carried over the failed link switches to the remaining member ports within the port channel.

2. If you choose **Existing Port Channel**:
   - Click the search icon next to the **Port Channel Id** field to select the Port channel ID for the device peer link.
   - From the list of port channels for the device, check the **Port Channel ID** check box.
   - Click **OK**.

     The Port channels selected for the device is displayed in the below area. The interfaces and the port channel to which they are connected to are displayed in the **Existing Port Channel** under the **Configure Secondary Device Peer Link** area.

3. If you choose **Create New Port Channel**:
   - In the **Port Channel Id** field, enter the port channel number for each device that you want to use as the vPC peer link.

     You can use different numbers for the two port channels on the two vPC devices that you are designating as the vPC peer link.
   - In the interface table below, choose the interfaces that you want to use for the vPC peer link.

Click **Next** to configure peer link port-channel setting.

Step 5 On the Configure Peer-Link Port Channel Settings screen:

Edit the Description, Port Mode and Native VLAN for the primary and the secondary devices. We recommend that you configure the Layer 2 port channels that you are designating as the vPC peer link in trunk mode and use two ports on separate modules on each vPC peer device for redundancy.

If you did not check the **Enable lacp on peer link** in the Select Devices screen, the Protocol field will display NONE.

If you want to create VLANs, the **Allowed VLANs** value must be a valid VLAN ID or range.

Click **Next** to view the summary information.

Step 6 On the **Summary** screen:

You can view the CLI configuration for the for the Primary Switch and Secondary Switch.

You can copy and save the configuration this configuration to your local directory.

Step 7 Click **Previous** to change any configurations.

Step 8 Click **Deploy** to configure vPC Peers.

After the deployment is complete, a status message shows whether the deployment is successful or a failure. Click **Know More** to view the status of each command deployed.

Delete vPC Peer

You can delete the vPC peer by clicking the **Delete vPC Peer** icon in the toolbar.

Procedure

Step 1 From the menu bar, choose **Configure > Deploy > vPC Peer** tab.

Step 2 Select the vPC domain which you want to delete, and click the **Delete vPC Peer** icon in the toolbar.

Click **Yes** when the confirmation window pops out.

Edit vPC Peer Configuration

You can edit the vPC domain by clicking the **Edit vPC Peer** icon in the toolbar.

Procedure

Step 1 From the menu bar, choose **Configure > Deploy > vPC Peer** tab.

Step 2 Select the vPC domain which you want to edit, and click the **Edit vPC Peer** icon in the toolbar.

You can edit the vPC Peer configuration by following the wizard as Add vPC Peer Wizard, on page 3.

Configuring vPC

After you finish configuring the vPC Peers, navigate to **Configure > Deploy > vPC** to configure the vPC.

You can view the history of tasks that are performed, navigate to **Configure > Deploy > vPC > History**. For more information, see vPC History, on page 6.

You can view the list of virtual port-channels (vPC) in the **Virtual Port-Channel(vPC)** table.

Table 3: Virtual Port-Channel(vPC)

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.
Primary vPC Peer-Device Name	Displays the vPC Primary device name.
Primary vPC Peer - Port Channel	Displays the vPC port channel for the primary vPC device that is connected to the multi-chassis endpoint or access switch.
Primary vPC Peer - Peer Port Channel	Displays the peer-link port channel for the vPC primary device.

Column	Description
Primary vPC Peer - Operational Mode	Displays the operational mode of the primary vPC endpoints.
Secondary vPC Peer - Device Name	Displays the vPC secondary device name.
Secondary vPC Peer - Port Channel	Displays the vPC port channel for the secondary device that is connected to the multi-chassis endpoint or access switch.
Secondary vPC Peer - Peer Port Channel	Displays the peer-link port channel for the vPC secondary device.
Secondary vPC Peer - Operational Mode	Displays the operational mode of the secondary vPC endpoints.
Multi Chassis vPC EndPoints - Device Name	Displays the multi-chassis vPC endpoints for each vPC ID under a vPC domain.
Multi Chassis vPC EndPoints - Port Channel ID	Displays the port channel on multi chassis vPC devices or access devices connected to the vPC peer switches.
vPC Consistency	Displays the vPC Consistency status. Corresponds vPC port channel and vPC.

This feature supports add, delete, and edit option for vPC.

vPC History

To view the deployed jobs on the created vPC peers, navigate to **Configure > Deploy > vPC > History** tab. You can view the list **vPC Peer History** information in the table.

Table 4: vPC Peer History

Column	Description
vPC Id	Specifies the domain ID for the vPC peer.
Primary Switch	Specifies the Primary Switch associated with the vPC.
Secondary Switch	Specifies the Secondary Switch associated with the vPC.
Access Switch	Specifies the Access Switch associated with the vPC.
Created By	Specifies the DCNM username who deployed this task.
Started At	Specifies the time at which the task was performed on the vPC peer. The time is displayed in the format YYYY-MM-DD HH:MM:SS.
Task Performed	Specifies the task that is performed on the vPC.
Status	Species the status of the task that is performed on the vPC.
View Command History	Select an activity, click **View Command History**. The **Command History** page displays the commands that are executed, status and error message for every command on the **Primary Switch**, **Secondary Switch**, and **Access Switch**, in their respective tabs.

Column	Description
Delete vPC Job	Select a vPC history and click **Delete** to delete the task history.

Add vPC

You can launch the vPC configuration wizard by clicking the **Add vPC** icon in the toolbar.

Procedure

Step 1 From the menu bar, choose **Configure > Deploy > vPC** tab.

Step 2 Click the **Add vPC** icon in the toolbar.

You are directed to the vPC creation wizard. There are five steps to complete the vPC creation.

Note Before configuring vPC we need to configure vPC domain. Once the Domain is configured, we can select the vPC peer, to create vPCs.

Step 3 In the Select Devices page, click on search button next to the Primary Switch text box to open a list of vPC peers.

After selection, click OK. Once the domain is selected the vPC domain page gets pre-populated with vPC domain information.

Note You cannot select a peer link if a switch associated is not a licensed device with configured LAN credentials.

Click **Ok**.

Step 4 In the **vPC ID** field, enter the value for this vPC.

By default, this field is auto-populated when selecting Devices.

Select the option to **Configure Access Switch/Fex**, **Configure New Fex** or **Configure Host** and specify the **Access Switch/Fex**.

A dual-home FEX will be created after you successfully deploy the vPC.

Step 5 To enable LACP on VPC port-channels, check **Create LACP Based Port Channels For Setting Up vPC** checkbox.

Note LACP based port-channel will be created. By default, LACP is not enabled on vPC port channel. We recommend that you create and use LACP for all these port channels. If you do not want to use LACP, deselect the option. Ensure that the LACP is configured with active mode on the interfaces on each port channel on the vPC peer devices. This configuration allows you to more easily detect compatibility between devices, unidirectional links, and multihop connection, and provides dynamic reaction to run-time changes and link failures.

Step 6 In the Configure links with vPC Primary and vPC Secondary page, configure the port channel for the Primary and Secondary vPC.

Step 7 Select or create the port-channel to configure the vPC. Click **Existing Port Channel** or **Create New port Channel** radio button to configure port channel.

A port channel bundles physical links into a channel group to create a single logical link that provides the aggregate bandwidth of up to 8 physical links on the M series module. If a member port within a port channel fails, the traffic previously carried over the failed link switches to the remaining member ports within the port channel.

- If you choose **Existing Port Channel**:
  1. Click the search icon next to the **Port Channel Id** field to select the Port channel ID for the device peer link.

     All the discovered port channels is displayed. The non-LACP port channel will be disabled and you cannot select only LACP enabled Port-channels.
  2. From the list of port channels for the device, check the **Port Channel ID** check box.
  3. Click **OK**.

     The Port channels selected for the device is displayed in the below area. The interfaces and the port channel to which they are connected to are displayed in the **Existing Port Channel** under the **Configure Secondary Device Peer Link** area.

- If you choose **Create New Port Channel**:
  1. In the **Port Channel Id** field, enter the port channel number for each device that you want to use as the vPC peer link.

     This field is auto-populated by default.

     You can use different numbers for the two port channels on the two vPC devices that you are designating as the vPC peer link.
  2. In the interface table below, choose the interfaces that you want to use for the vPC peer link.

Click **Next** to review and modify other vPC port channel settings.

Step 8 In the Configure vPC Port Channel Settings, review and configure parameters for the port channel for both Primary and Secondary switches.

Edit the Description, Port Mode, Native VLAN and Protocol for the port channels of the primary and the secondary devices.

If you did not check the **Create LACP based Port Channels for setting up vPC** in the Select Devices screen, the Protocol field will display NONE.

If you want to create VLANs, the **Allowed VLANs** value must be a valid VLAN ID or range.

Click **Next**.

Step 9 In the**Summary** page, you can view the summary of your configuration for the Primary Switch, Secondary Switch, and Access Switch.

You can copy and save the configuration this configuration to your local directory.

Step 10 Click **Previous** to change any configurations.

Step 11 Click **Deploy** to configure vPC on the devices.

After the deployment is complete, a status message shows whether the deployment is successful or a failure. Click **Know More** to view the status of each command deployed.

Delete vPC

You can delete the virtual Port-Channel by clicking the **Delete vPC** icon in the toolbar.

Procedure

Step 1 From the menu bar, choose **Configure > Deploy > vPC** tab.

Step 2 Select the vPC which you want to delete, and click the **Delete vPC**icon in the toolbar.

Click **Yes** when the confirmation window pops out.

Edit vPC Configuration

You can edit the vPC configuration by clicking the **Edit vPC** icon in the toolbar.

Procedure

Step 1 From the menu bar, choose **Configure > Deploy > vPC** tab.

Step 2 Select the vPC which you want to edit, and click the **Edit vPC** icon in the toolbar.

You can edit the selected vPC configuration by following the Add vPC, on page 7.

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.

Step 4 Create, Publish, and Deploy Cable Plans.

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.

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 5: 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 5: DCHP Scopes display fields, on page 10.

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.

Procedure

Step 1 From the menu bar, select **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

Procedure

Step 1 From the menu bar, select **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 6: 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

Perform the following task to add an image or a configuration server URL:

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 Click 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

Perform the following task to edit an image or a configuration server URL to the repository.

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

Perform the following task to delete an image or a configuration server URL to the repository.

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.

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

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 16 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

Procedure

Step 1 From the menu bar, select **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 Modify/View template icon.
Step 4 Edit the template content and click **Save** to save the template or **Save and Exit** to save and exit the screen.

Cloning a Template

Procedure

Step 1 From the menu bar, select **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

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

Procedure

Step 1 From the menu bar, select **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.

Procedure

Step 1 From the menu bar, select **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 7: Annotation Keys

Key Name	Default Value	Description
DisplayName	Empty String	The value is displayed as a variable label in the template form GUI, on POAP definition screen.
Description	Empty String	Displays the description next or below the template variable field in the template form GUI.

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

Fields and Icons	Description
Icons	
Add	Allows you to add a POAP definition. For more information, see Creating a POAP definition, on page 19.
Edit	Allows you to edit a POAP definition. For more information, see Editing a POAP Definition, on page 21.
Delete	Allows you to delete a POAP definition. For more information, see Deleting POAP Definitions, on page 21.
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 21.
Change Image	Allows you to change the image for the defined POAP definition. For more information, see Change Image, on page 22.
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.
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

Procedure

Step 1 From the menu bar, select **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 on **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 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 User Name and Switch Password.

Step 10 Click **Next** to Select the Switch Config Template.

Step 11 Use the drop-down to select the Template and click View to specify the Template Parameters.

Step 12 Enter Template Parameters.

Step 13 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

Procedure

Step 1 From the menu bar, select **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 19 and Uploading a POAP Definition, on page 20 sections.

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

Deleting POAP Definitions

Procedure

Step 1 From the menu bar, select **Configure > Deploy > POAP > POAP Definitions**.

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

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

Procedure

Step 1 From the menu bar, select **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 need to change the image. Click **Change Image**.

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

The Multi Device Image Change screen appears.

Step 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 will replace 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

Procedure

Step 1 From the menu bar, select **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 he Inter-Switch Links between existing switches 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

Procedure

Step 1 From the menu bar, select **Configure > Deploy > POAP > Cable Plan**.

Step 2 Click **Delete** from DCNM.

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

Deploying a Cable Plan

Procedure

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

Revoking a Cable Plan

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 submenu:

Template Library

The Template Library menu includes the following submenus:

Template Library

Cisco DCNM allows you to add, edit, or delete user-defined templates that are configured across different Cisco Nexus and Cisco MDS platforms. The following parameters are displayed for each template that is configured on the Web UI of the Cisco DCNM **Configure > Templates > Template Library > Templates**. 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 8: 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 tot 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.

Table 9: Templates Table Field and Description

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.
Implements	Displays the abstract template to be implemented.
Dependencies	Specifies the specific feature of a switch.

Field	Description
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.
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. You can click on the Help icon next to the Template Content window for information about editing the content of the template. Click on the Help icon next to the Template Content window for information about editing the content of the template.

This section contains the following:

Template Format

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

Property Name	Description	Valid Values	Optional?
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, All 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_ETHERNET
		  • INTERFACE_BD
		  • INTERFACE_PORT_CHANNEL
		  • INTERFACE_MGMT
		  • INTERFACE_LOOPBACK
		  • INTERFACE_NVE
		  • DEVICE
		  • FEX
		  • INTERFACE
		• SHOW
		  • VLAN
		  • INTERFACE_VLAN
		  • INTERFACE_VPC
		  • INTERFACE_ETHERNET
		  • INTERFACE_BD
		  • INTERFACE_PORT_CHANNEL
		  • INTERFACE_FC
		  • INTERFACE_MGMT
		  • INTERFACE_LOOPBACK	

Property Name	Description	Valid Values	Optional?
		• INTERFACE_NVE • DEVICE • FEX • INTERFACE • PROFILE • VXLAN • FABRIC • NA • ABSTRACT • VLAN • INTERFACE_VLAN • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORT_CHANNEL • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • DEVICE • FEX • 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
timestamp	Shows the template modified time	Modified date and time in the format YYYY-MM-DD HH:MM:SS	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?
string	Free text `Example: Description for the variable`	No
boolean	true|false	No
enum	`Example: running-config, startup-config`	No
float	Floating number format	No
Integer	Any number	No
ipAddress	IPv4 OR IPv6 address	No
ipV4Address	IPv4 address	No
ipV6Address	IPv6 address	No
ipV4AddressWithSubnet	`Example: 192.168.1.1/24`	No
ipV4AddressWithSubnet	`Example: 1:2:3:4:5:6:7:8/22`	No
ipV6AddressWithPrefix	`Example: 1:2:3:4:5:6:7:8` `22`	No

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

macAddress	14 or 17 character length MAC address format	No
interface	Format: <if type><slot>[/<sub slot>]/<port> `Example: eth1/1, fa10/1/2 etc.`	No
integerRange	Contiguous numbers separated by "-" Discrete numbers separated by "," `Example: 1-10,15,18,20`	Yes
floatRange	`Example: 10.1,50.01`	Yes
ipV4AddressRange	`Example: 172.22.31.97 - 172.22.31.99, 172.22.31.105 - 172.22.31.109`	Yes
interfaceRange	`Example: eth10/1/20-25, eth11/1-5`	Yes

Variable Type	Valid Value	Iterative?
string[]	`Example: {a,b,c,str1,str2}`	Yes
ipAddress[]	`Example:{192.168.1.1, 192.168.1.2, 10.1.1.1}`	Yes
wwn (Available only in the Web Client)	`Example: 20:01:00:08:02:11:05:03`	No

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
string	literal string	Yes									Yes	Yes	Yes
boolean	A boolean value. Example: true	Yes											
enum			Yes										
float	signed real number. Example: 75.56, -8.5	Yes	Yes	Yes	Yes	Yes							
integer	signed number Example: 50, -75	Yes	Yes		Yes	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	IP address in IPv4 or IPv6 format	Yes											
ipV4Address	IPv4 address	Yes											
ipV6Address	IPv6 address	Yes											
ipV4AddressWithSubnet	IPv4 Address with Subnet	Yes											
ipV6AddressWithPrefix	IPv6 Address with Prefix	Yes											
ipAddressWithOptionalPrefix	IPv4 or IPv6 Address (does not require prefix/subnet)												
macAddress	MAC address												
interface	specifies interface/port Example: Ethernet 5/10	Yes	Yes				Yes	Yes	Yes	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
integerRange	Range of signed numbers Example: 50-65	Yes	Yes		Yes	Yes							
floatRange	range of signed real numbers Example: 50.5 - 54.75	Yes	Yes	Yes	Yes	Yes							
ipV4AddrRange		Yes											
interfaceRange		Yes	Yes				Yes	Yes	Yes	Yes			
string[]	string literals that are separated by a comma (,) Example: {string1, string2}	Yes											
ipAddress[]	List of IP addresses separated by a comma (,)	Yes											
wwn	WWN 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
struct	Set of parameters that are bundled under a single variable.												

Example: Meta Property Usage

```
##template variables

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

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

##
```

Variable Annotation

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

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

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

Annotation Key	Valid Values
DisplayName	Text **Note** Enclose the text with quotes, if there is space.
Description	Text
IsManagementIP	"true" or "false" **Note** This annotation must be marked only for variable "ipAddress".
IsDeviceID	"true" or "false"

Annotation Key	Valid Values
IsInternal	“true” or “false”
IsMandatory	“true” or “false”
UsePool	“true” or “false”
Username	Text
Password	Text
DataDepend	Text

Example: Variable Annotation

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

Example: IsMandatory Annotation

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

IsShowAnnotation

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

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]**

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.

Step 3 Specify a **Template Name**, **Template Description**, **Tags**, **Implements**, and **Dependencies** for the new template.

Step 4 Select the supported platforms that the template must support.

Step 5 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 6 Select a **Template Sub Type** and **Template Content Type** for the template, and select **Published** to make the template read-only. You cannot edit a published template.

Step 7 Click **Template Content** to edit the template syntax. For information about the structure of the Configuration Template, see the *Template Structure* section.

Step 8 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 9 Click **Validate Template Syntax** to validate the template values.

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

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.

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

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

Configuring Template Job

You can configure and schedule jobs for individual templates from the **Configure > Templates > Template Library > Templates** page.

Procedure

Step 1 Select a template.

Note Config job wizard is applicable only for CLI templates.

Step 2 Click the **Launch job creation wizard** icon and click **Next**.

Step 3 Use the drop-down to select **Device Scope**.

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

Note If no devices are displayed, check if the device LAN credentials are configured from Cisco DCNM **Web Client > Administration > Credentials Management > LAN Credentials**.

Step 4 Use the arrows to move the devices to the right column for job creation and click **Next**.

Step 5 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 will vary.

Step 6 In the **Edit Variable Per Device** section, double click the fields to edit the variables for specific devices and click **Next**.

Step 7 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 8 Specify a job name and description.

The Device Credentials will be populated from **Administration > Credentials Management > LAN Credentials**.

Step 9 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 10 Use the check box to select **Copy Run to Start**.

Step 11 If you want to configure additional transaction and delivery options, use the check box to select **Show more options**.

Step 12 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 13 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 14 Click **Finish** to create the job.

A confirmation message is displayed that the job has been successfully created.

Modifying a Template

You can edit the user-defined templates. However, the 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

You can copy templates.

Procedure

Step 1 From **Configure > Templates > Template Library > Templates**, 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 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 pre-defined templates. From Cisco DCNM Release 11.0(1), you can delete multiple templates at once.

Procedure

Step 1 From the menu bar, select **Configure > Templates > Template Library > Templates**.

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

The template will be deleted without any warning message.

What to do next

The template will be deleted from the list of templates on the Web Client. However, when you restart the DCNM services, the deleted templates will be displayed on the **Configure > Templates > Template Library > Templates**.

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

Importing a Template

Perform the following task to import a template to the Cisco DCNM.

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, on page 45.

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 43.

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.

Exporting a Template

Procedure

Step 1 From the menu bar, select **Configure > Templates > Template Library > Templates**.

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

The browser will request 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 www.cisco.com/go/dcnm, and download the latest 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

Procedure

Step 1 From the menu bar, select **Configure > Templates > Templates Library > Jobs**.

The jobs are listed along with the Job ID, description and status.

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 Excecution 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 10: 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 11: 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.

Field	Description
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.

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.

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**.

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

Field	Description
User	Specifies the who created this job.
Group	Specifies the group to which this job belongs.
Group Job	
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.

Archive Jobs

You can add, delete or view the job.

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 To add a job, from the Cisco DCNM home page, 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 will be 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.

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.

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**.

What to do next

You can also configure the Cisco DCNM to retain the number of archived files per device. From Cisco DCNM home page, 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

Field	Description
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.

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 12: 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 viewa configuration file.

Table 13: 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

This feature allows you to 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.

Perform the following task to compare configuration files.

Procedure

Step 1 In the Cisco DCNM home page, choose **Configure > Backup > Archives**.

Step 2 In the **Archives** area, click the arrow 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 you select is designated as 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. From the drop-down list in the right-top corner, choose **All** to view the entire configuration or 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—Newly 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

The Image Management menu includes the following submenus:

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. 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
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.
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

Perform the following task to upgrade the devices that are discovered by Cisco DCNM.

Procedure

Step 1 Choose **Configure > Image Management > Upgrade [ISSU] > Upgrade History**, click **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 2 Select the check box to the left of the switch name.

You can select more than one device and move the devices to the right column.

Step 3 Click **Add** or **Remove** icons to include the appropriate switches for upgrade.

The selected switches appear in a column on the right.

Step 4 Click **Next** to navigate to **Specify Software Images** window. This tab displays the switches that you selected in the previous screen and allows you to choose the images for upgrade.

- The **Auto File Selection** check box enables you to specify a file server, an image version, and a path where you can apply the upgrade 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 with respect to the FTP or TFTP home directory if you choose FTP or TFTP. Specify the absolute path of the image if you are using TFTP server that is provided by Cisco DCNM, local DCNM TFTP. You cannot use the same DCNM TFTP server for creating another job when the current job is in progress.

Step 5 Click **Select Image** in the **Kickstart image** column.

Software Image Browser screen appears.

Note
- Cisco Nexus 3000 series switches and Cisco Nexus 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 will be disabled.
- If there is an issue in viewing the **Software Image Browser** screen, reduce the font size of your browser and retry.

Step 6 Click **Select Image** in the **System Image** column.

Software Image Browser screen appears.

Step 7 On the **Software Image Browser** screen, you can choose the kickstart 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 kickstart 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 kickstart 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.

c) Click **OK** to choose the kickstart image or **Cancel** to revert to the **Specify Software Images** page.

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.
b) Click **OK** to choose the kickstart image or **Cancel** to revert to the **Specify Software Images** page.

Step 8 The **Vrf** column indicates the name of the virtual routing and forwarding (VRF).

VRF is not applicable for Cisco MDS devices.

Step 9 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 is shown and marked as KB).

Bootflash browser shows the file name, 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 10 **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 11 Drag and drop the switches to reorder the upgrade task sequence.

Step 12 Select **Skip Version Compatibility** if you are sure that the version of the Cisco NX-OS software on your device is compatible with the upgrade images that you have selected.

Step 13 Select **Select Parallel Line Card upgrade** to upgrade all the line cards at the same time.

Upgrading a parallel line card is not applicable for Cisco MDS devices.

Step 14 Select **Options** under the **Upgrade Options** column to choose the type of upgrade.

Upgrade Options window appears with two upgrade options. The drop-down menu for **Upgrade Option 1** has the following options:

- **NA**
- **bios-force**
- **non-disruptive**

NA is the default value.

The drop-down menu for **Upgrade Option 2** has the following options:

- **NA**
- **bios-force**

When **NA** is selected under **Upgrade Option 1**, **Upgrade Option 2** is grayed out. When **bios-force** is selected under **Upgrade Option 1**, **NA** is the only option under **Upgrade Option 2**. 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 switches and Cisco Nexus 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 15 Click **Next**.

If you did not 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 taken to check the compatibility of the image 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 16 Click **Finish Installation Later** to perform the upgrade later.

Step 17 Click **Next**.

Step 18 Check the **Next** check box to put a device in maintenance mode before upgrade.

Step 19 Check the check box to save the running configuration to the startup configuration before upgrading the device.

Step 20 You can schedule the upgrade process to occur immediately or later.

1. Select **Deploy Now** to upgrade the device immediately.
2. 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 21 You can choose the execution mode based on the devices and the line cards you have chosen to upgrade.

1. Select **Sequential** to upgrade the devices in the order in which they were chosen.
2. Select **Concurrent** to upgrade all the devices at the same time.

Step 22 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.

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.

1. Select **Deploy Now** to upgrade the device immediately.
2. 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 based on the devices and the line cards that you have chosen to upgrade.

1. Select **Sequential** to upgrade the devices in the order in which they were chosen.
2. Select **Concurrent** to upgrade the devices at the same time.

Step 7 Click **Finish** to complete the upgrade process.

View

Perform the following task to view the status of tasks.

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**.

Installation Task Details window appears.

Step 3 Click **Settings**. Select **Columns** and choose the column details options.

This window displays the location of the kickstart and system images, compatibility check status, installation status, descriptions, and logs.

Step 4 Select the device.

The detailed status of the task is displayed below. For the completed tasks, the response from the device is displayed.

If the upgrade task is in progress, a live log of the installation process appears.

Note This table is refreshed every 30 secs for jobs in progress, when you are on this window.

The switch-level status for an ongoing upgrade on a Cisco MDS switch is not displayed for other users without SAN credentials applied. To apply SAN Credentials, choose **Administration > Credentials Management > SAN Credentials**.

Delete

Perform the following task to delete a task.

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 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.
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.

Patch [SMU]

The Patch [SMU] menu includes the following submenus:

Patch 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 will be listed in 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.

Field	Description
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

Perform the following task to install the patch on your devices using Cisco DCNM.

Procedure

Step 1 Choose **Configure > Image Management > Patch [SMU] > Installation History**, click **Install**.

The **Select Switches** window appears. All the Cisco Nexus licensed switches that are discovered by Cisco DCNM are displayed.

Step 2 Select the check box to the left of the 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 hand column.

Step 4 Click **Next**.

Step 5 Click **Select Packages** in the **Packages** column.

SMU Package Browser screen appears.

Step 6 In the **SMU Package Browser** screen, 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 at **Configure > Image Management > Repositories** are displayed in the drop-down list.

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.

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.

b) Click **OK** to choose the image, **Clear Selections** to uncheck all the check boxes, or **Cancel** to revert to the **SMU Package Browser** screen.

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, on the **DCNM > Inventory > Switches** window.

Uninstall Patch

Perform the following task to uninstall the patch on your devices using Cisco DCNM.

Procedure

Step 1 Choose **Configure > Image Management > Patch [SMU] > Installation History**, click **Uninstall**.

The **Select Switches** page appears. Cisco Nexus licensed switches that are discovered by Cisco DCNM 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

Perform the following steps to delete the patch installation tasks.

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 the licensed 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 Cisco Nexus 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.
IP Address	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.

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 only one package file to be installed on the device.

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 only one package file to be installed on the device.

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**.

Choose **Inventory > Switches** to view the list of packages that are installed on the switch.

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]

Perform the following task to uninstall the RPM on your devices using Cisco DCNM.

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

Perform the following tasks to delete the package installation tasks from the history view.

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 licensed switches.If there are multiple RPM packages that are installed on the switch, the names of the packages are separated by commas.

Click **Refresh** to refresh the table.

Maintenance Mode [GIR]

The Maintenance Mode [GIR] menu includes the following submenus:

Maintenance Mode [GIR]

This feature 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.

Field	Description
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.
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.

Repositories

This feature allows you to add image servers and configuration servers information to fetch images for Upgrade, Patch, and POAP mode operations.

You can specify valid servers for SCP/SFTP/FTP/TFTP. DCNM does not perform the validation for SCP/SFTP/FTP/TFTP servers while creating or updating the servers. DCNM performs validation only for the SCP servers.

Note The SCP repositories use SSH protocol for the directory listing and therefore you need to enable SSH on the SCP repository server. The SFTP repository uses SFTP protocol for directory listing. The TFTP and FTP repositories do not support directory listing. You need to specify the file path manually.

Add Image or Configuration Server URL

Perform the following task to add an image or a configuration server URL to the repository.

Procedure

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

The **Add Image or Configuration Server URL** window appears.

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.

Step 5 Specify the username and password.

Step 6 Click **OK** to save.

Deleting an Image or Configuration Server URL

Perform the following task to delete an image from the repository.

Procedure

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

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

Note The default SCP Repository cannot be deleted.

Editing an Image or Configuration Server URL

Perform the following task to edit an image or a configuration server URL to the repository.

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

Perform the following task to upload different types of images to the server. Devices use these images during POAP.

Procedure

Step 1 On the **Image and Configuration Servers** window, check the server name check box to select the server for uploading images.

The **Select Image File** window appears.

Step 2 Click **Browse** to select the image file from the directory.

Step 3 From the **Platform** drop-down list, select the device to which you need to upload this image.

Step 4 From the **Type** drop-down list, select the type of the image you are uploading to the device.

Step 5 Click **OK**.

The image is uploaded to the repository.

Streaming Telemetry for LAN Deployments

In today's data center environments, granular visibility and tracking of network events has become critical. The traditional polling-based methods that pull network state in predefined intervals need a fork-lift upgrade. More advanced streaming approaches are required that provide network event visibility in closer to real time through a push method. Streaming telemetry not only allows data to be pushed out at a much finer granularity with a lower cadence (shorter interval) but it also enables event-based notifications. While getting relevant data in a timely fashion is highly desirable, the data needs to be analyzed and converted into actionable insights.

As a first step toward LAN analytics, DCNM 11.0(1) enables subscriptions for environmental metrics through streaming telemetry for consumption and analysis. The environmental metrics that are streamed include CPU, Memory, Power, Temperature, and Fan Speed; all these are enabled with a single click. DCNM allows you to configure the streaming interval for these metrics. The default streaming interval for CPU, Memory is set to 30 seconds, and those for Power, Temperature, and Fan Speed is set to 300 seconds (5 minutes). The per-metric real-time streaming dashboards allow filtering on a per fabric and per switch level including a per-switch drill-down where applicable. Streaming telemetry is currently supported on the Nexus 9000 platforms.

Pre-requisites for Enabling the LAN Telemetry Feature

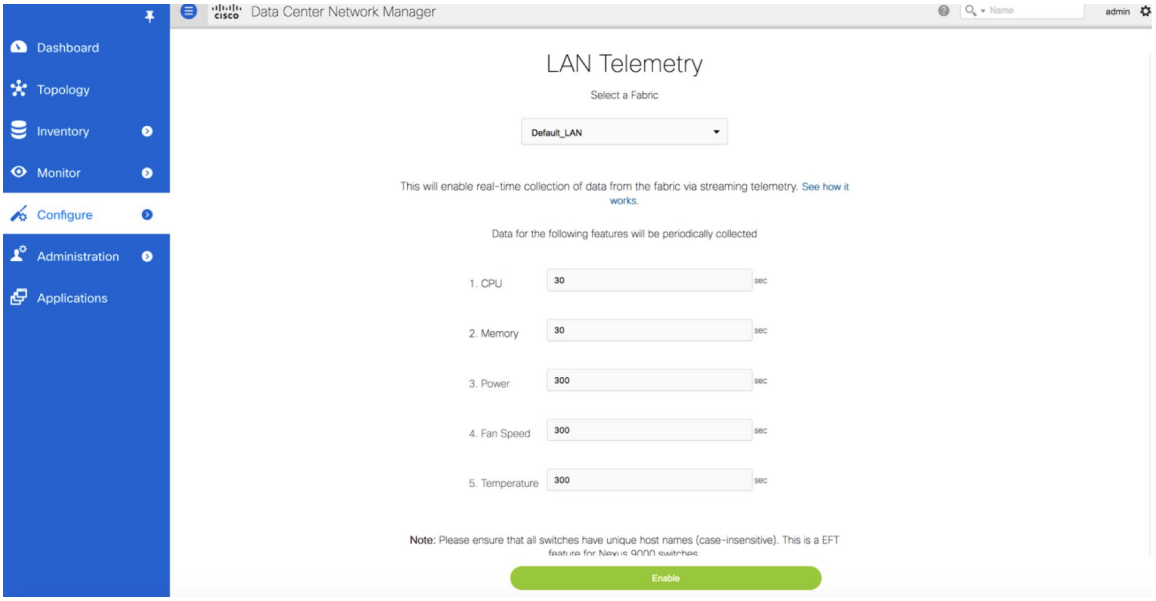
The pre-requisites for enabling this feature are:

- The Cisco Nexus 9000 switches and Cisco DCNM need to be time synchronized (NTP is recommended).
- Minimum software version on the Nexus 9000 switches must be 7.0(3)I6(1) or higher.

Enabling the Streaming Telemetry Feature

Procedure

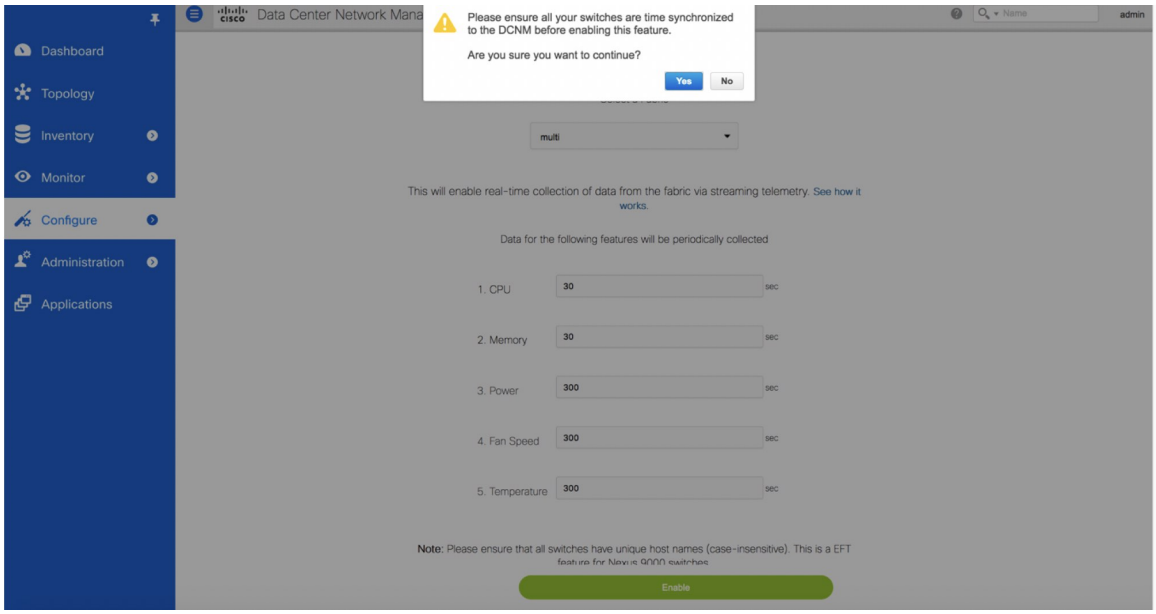
Step 1 Choose **Configure > LAN Telemetry > Configure**. Select the fabric for which LAN Telemetry has to be enabled. Then press the **Enable** button.



A warning message appears to indicate that the Cisco DCNM and switches need to be time-synchronized before this feature is enabled. Recall, that this is a prerequisite for this feature. If the prerequisite is met, acknowledge by clicking **Yes**.

Note When Telemetry is enabled, the NTP configuration is done on the switches for LAN Classic deployment, wherein the NTP server address is set to DCNM's out-of-band interface's IPv4 address. In case of HA setups, the NTP server address is set to the VIP address of the out-of-band interface.

Ensure that the NTP configurations are not removed/modified from the switches.



Step 2 Once this feature is enabled, a message appears indicating the initialization process has begun, which takes a couple of minutes. This time is needed for the streaming configuration to be pushed to the switches. The initial data to be streamed out from the switches, which are consumed by DCNM, and depicted on the LAN telemetry dashboard.

Once the LAN telemetry preview feature is enabled, DCNM updates the switch telemetry configuration for the environmental metrics. Every switch that does not conform to the telemetry requirements (must be Cisco Nexus 9000) is excluded from the configuration update. The status of the switch configuration can be monitored by choosing **Configure > LAN Telemetry > Health**. In case of Easy Fabric, it can be monitored by choosing **Control > LAN Telemetry > Health**.

Once the jobs are successfully executed, the required telemetry configuration has been applied to the switches and the streaming data appears once received and processed.

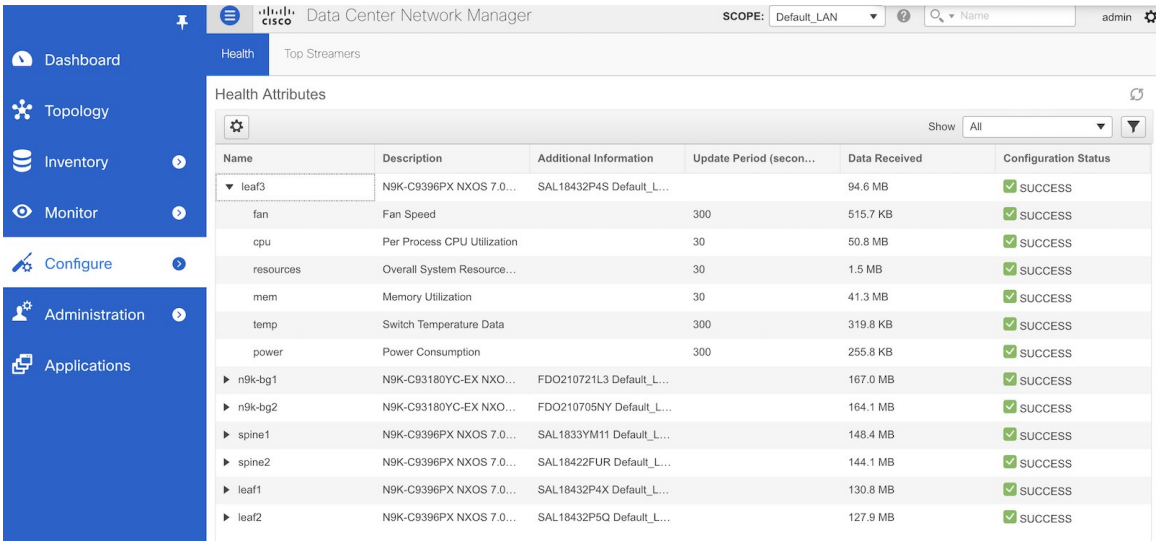
Viewing LAN Telemetry Health

The LAN Telemetry Health window provides a detailed break-down of how much data is streamed out by each switch per feature for the last 24 hours. This window shows the status of the configuration for every switch, apart from showing the statistics of the received data for every metric from every switch.

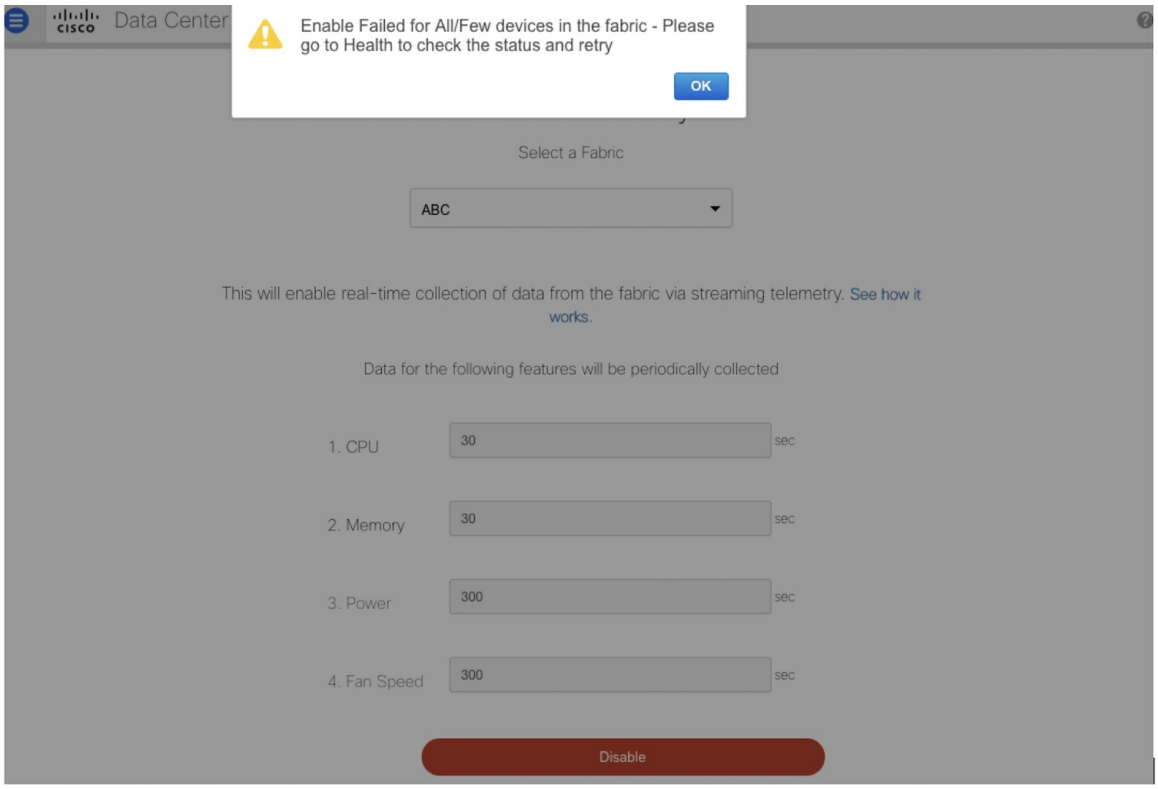
To view the LAN Telemetry Health, perform the following steps:

Procedure

Step 1 Choose **Configure > LAN > LAN Telemetry > Health**.



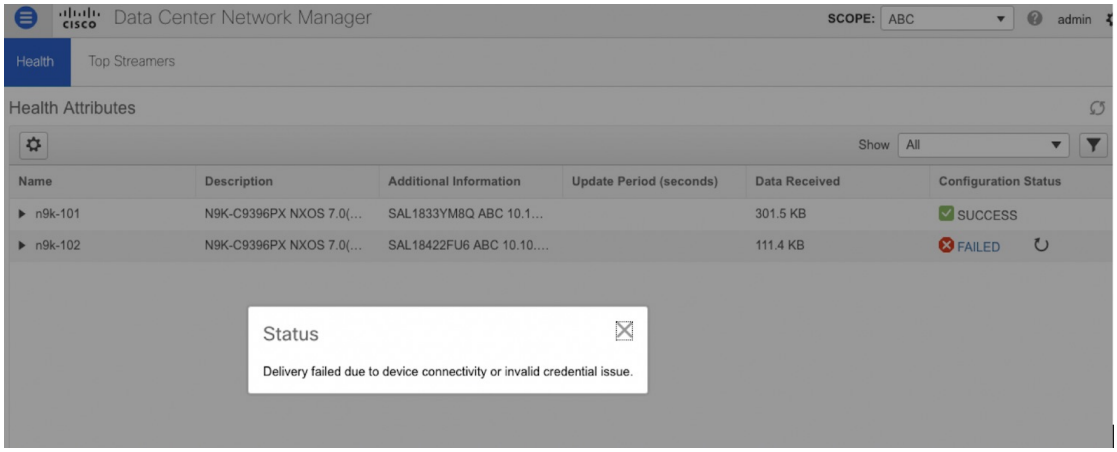
When Telemetry is enabled or disabled, there is a chance that enabling or disabling can fail in some or all the switches. When that happens, a pop-up similar to the following screen appears.



There are two possible options:

1. You can go to the Health page, and retry the configuration for those switches that failed. When a configuration cannot be applied or removed on any switch, **Configuration Status** in the health page, appears as FAILED. Upon clicking the 'FAILED' link, a pop-up would show the reason for the failure.

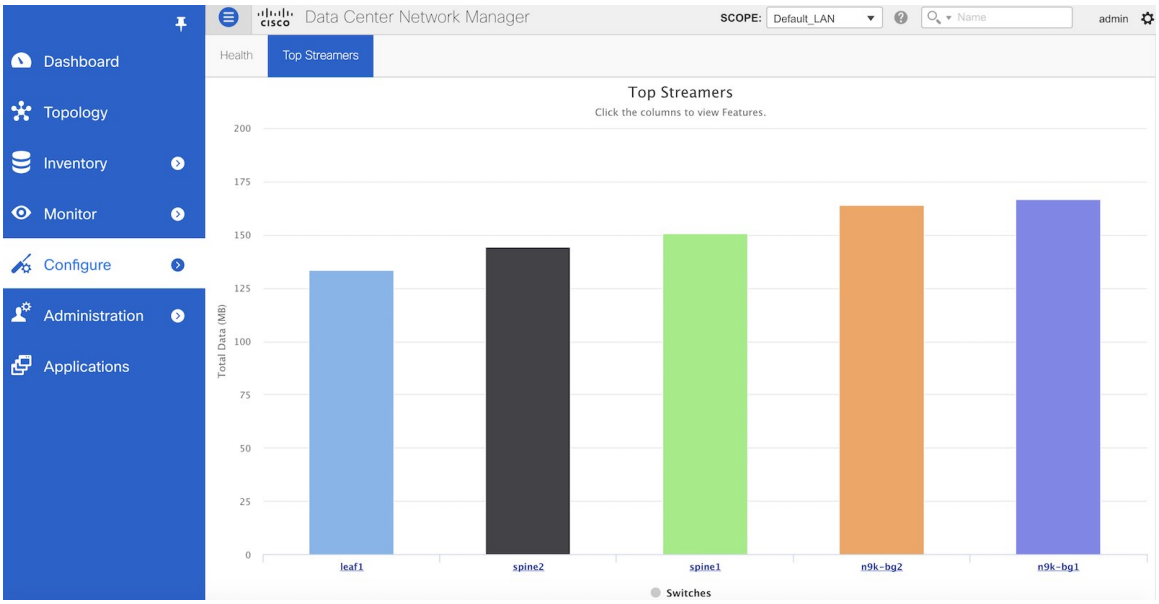
After you correct the failure, the configuration can be retried by clicking on the retry button appearing next to the Configuration Status for every switch. The screen-shot for that is also shown below.



2. You can stay in the main Telemetry > Configure page. It would display a dialogue box with the failed message. Then you can reverse the configuration for the successfully configured switches. In other words:
   - When “Enable” fails for some or all switches, the screen has a Red button with “disable” option. This means, for those switches, wherein enabling Telemetry was successful, you can disable Telemetry on those switches. If “Enable” failed on all switches, you will still see the Red button with “disable” option. Clicking on “disable” is a no-op. In both the cases, you will see the green button with the “enable” option in a few seconds after disabling is completed. This removes the “retry” option from the health page since you want to “disable” telemetry and there is nothing to retry.

3. Similarly, when “Disable” fails for some or all switches, the screen has a Green button with “Enable” option. This means, for those switches, wherein disabling Telemetry was successful, you can Enable Telemetry on those switches. If “Disable” failed on all switches, you will still see the Green button with “Enable” option. Clicking on “Enable” is a no-op. In both the cases, you will see the Red button with the “Disable” option in a few seconds after Enabling is completed. Doing this, removes the “retry” option from the health page since you want to “enable” telemetry and there’s nothing to retry.

Step 2 Click the **Top Streamers** tab to view the graphs that depicts the top five streaming switches and has a drill-down capability for a feature-wise break-down.



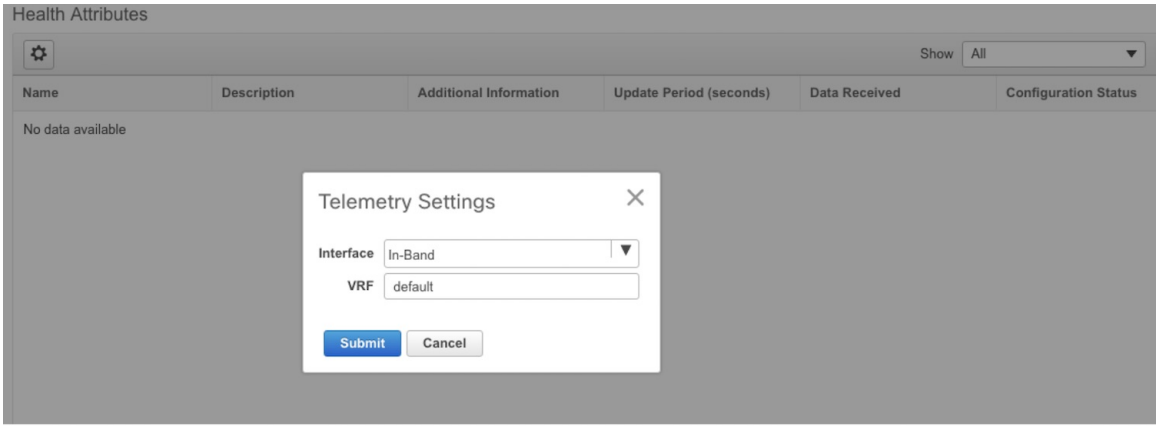
Telemetry Streaming Interface

Telemetry data, by default is streamed through the management interface of the switches to the Cisco DCNM. This is the Out-of-Bank network. This is a global configuration for all fabrics or switch-groups in DCNM. The switches can also stream the Telemetry data through their front panel ports to DCNM assuming there's connectivity from the switches to the DCNM. This is the In-band network. To use the in-band network, do the following:

Procedure

Step 1 Disable Telemetry on all the Enabled fabrics.

Step 2 Go to the Health page and change the Settings as shown in the figure below.



The VRF option is set to default. You can also change this to any other VRF assuming that the switches are configured with the VRF and there is availability to the in-band interface of the DCNM through that VRF.

Note If Telemetry is already enabled for some fabrics, you should first disable Telemetry on all the enabled fabrics and only then modify the Telemetry network setting. After modifying the Telemetry network settings, you can enable Telemetry on the fabrics. Now, Telemetry data start coming through the in-band interface.