



Configure

This chapter contains the following topics:

- [Deploy, on page 1](#)
- [Templates, on page 18](#)
- [Backup, on page 48](#)
- [Image Management, on page 60](#)
- [LAN Telemetry Health, on page 78](#)

Deploy

The Deploy menu includes the following submenus:

POAP Launchpad



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

The POAP launchpad contains the following configuration steps:

Procedure

-
- | | |
|---------------|--|
| Step 1 | Create and manage scopes for POAP creation. |
| Step 2 | Set a server for images and configuration files. |
| Step 3 | Generate from a template or upload existing configuration. |
-

Power-On Auto Provisioning (POAP)

Power-On Auto Provisioning (POAP) automates the process of upgrading software images and installing configuration files on Cisco Nexus switches that are being deployed in the network for the first time.

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

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

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

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

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

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

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



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

DHCP Scopes

DHCP scope is a well-defined term in DHCP arena. It is used to define a policy for giving out IP addresses and other options to host on a specific IP subnet. In DCNM, we use the DHCP 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 1: DHCP 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/Bootsript 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 1: DCHP Scopes display fields, on page 2](#).
 - Step 4** Click **OK** to add a DHCP scope.
-

Editing an existing DHCP Scope



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

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

Procedure

-
- Step 1** Choose **Configure > Deploy > POAP > DHCP Scopes**.
 - Step 2** Use the checkbox to select the DHCP scope.
 - Step 3** Click **Edit** scope icon.
 - Step 4** In the Edit DHCP Scope window, edit the DHCP scopes.
 - Step 5** Click **Apply** to save the changes.
-

Deleting a DHCP Scope

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

Procedure

-
- Step 1** Choose **Configure > Deploy > POAP > DHCP Scopes**.
 - Step 2** Use the checkbox to select the DHCP scope.

Step 3 Click Delete scope icon.

Step 4 In the delete notification, click **Yes** to delete the DHCP scope.

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

Image and Configuration Servers

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

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

The following table details the columns in the display.

Table 2: DHCP Scopes display fields

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

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

Add Image or Configuration Server URL

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

Procedure

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

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

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

Step 4 Enter Hostname/Ipaddress and Path.

Step 5 Specify the Username and Password.

Step 6 Click **OK** to save.

Editing an Image or Configuration Server URL

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

Procedure

-
- Step 1** On the Image and Configuration Servers page, select an existing Image and Configuration Server from the list, and click the **Edit** icon.
 - Step 2** In the **Edit Image or Configuration Servers URL** window, edit the required fields.
The Default_SCP_Repository cannot be edited.
 - Step 3** Click **OK** to save or click **Cancel** to discard the changes.
-

Deleting an Image or Configuration Server URL

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

Procedure

-
- Step 1** On the Image and Configuration Servers page, select an existing Image and Configuration Server from the list, and click the **Delete** icon.
 - Step 2** In the delete notification, click **Yes** to delete the image and configuration server.

Note The default SCP Repository cannot be deleted.

Using the File Browser

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

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

Procedure

-
- Step 1** On the Image and Configuration Servers page, select an existing Image and Configuration Server from the list.
 - Step 2** Click the **File Browser** button to see the file in the directory. The File browser pop-up dialog appears.
-

Uploading an Image File

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

Procedure

-
- Step 1** On the **Image and Configuration Servers** window, select an existing **Image and Configuration Server** from the list.
 - Step 2** Click the **Image Upload** button.
 - Step 3** Click the **Choose File** button to choose an image file.
 - Step 4** In the **Platform** drop-down list, choose the hardware model name of the managed device. For example, N7K, N9K.
 - Step 5** In the **Type** drop-down list, choose the image type. For example, kickstart, system.
-

POAP Templates

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

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

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

This section contains the following:

Add POAP Template

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

Procedure

-
- Step 1** Choose **Configure > Deploy > POAP > POAP Definitions**.
The **POAP Definitions** window is displayed.
 - Step 2** In the **Configuration Steps**, click the template hyperlink in the POAP Definitions section.
 - Step 3** Click the **Add template** icon.
 - Step 4** Specify the **Template Name**, **Template Description**, and **Tags**.
 - Step 5** Use the checkbox to specify the Supported Platforms.
 - Step 6** Select the template type from the drop-down list.
By default, CLI template type is selected.
 - Step 7** Select the **Published** checkbox if you want the template to have 'Read Only' access.
 - Step 8** In the **Template Content** pane, specify the content of the template.

For help on creating the template content, click the **Help** icon next to the Template Content header. For information about POAP template annotations, see the [POAP Template Annotation, on page 8](#) section.

- Step 9** Click **Validate Template Syntax** to validate syntax errors.
 - Step 10** Click **Save** to save the template.
 - Step 11** Click **Save and Exit** to save the template and exit the window.
 - Step 12** Click **Cancel** to discard the template.
-

Editing a Template

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

Procedure

- Step 1** Choose **Configure > Deploy > POAP > POAP Definitions**.
 - Step 2** In the Configuration Steps, click the template hyperlink in the POAP Definitions section.
 - Step 3** Select a template from the list and click the **Modify or View** template icon.
 - Step 4** Edit the template content and click **Save** to save the template or **Save and Exit** to save and exit the screen.
-

Cloning a Template

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

Procedure

- Step 1** Choose **Configure > Deploy > POAP > POAP Definitions**.
 - Step 2** In the Configuration Steps, click the template hyperlink in the POAP Definitions section.
 - Step 3** Select a template from the list and click **Save Template As** icon.
 - Step 4** Edit the template and click **Save** to save the template or **Save and Exit** to save and exit the screen.
-

Importing a Template

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

Procedure

- Step 1** Choose **Configure > Deploy > POAP**.
 - Step 2** Under **Configuration Steps**, click the template hyperlink in the **POAP Definitions** section.
 - Step 3** Select a template from the list and click **Import Template**.
 - Step 4** Select the template file and upload.
-

Exporting a Template

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

Procedure

-
- Step 1** Choose **Configure > Deploy > POAP > POAP Definitions**.
 - Step 2** In the Configuration Steps, click the template hyperlink in the POAP Definitions section.
 - Step 3** Select a template from the list and click **Export** template icon.
 - Step 4** Select a location for the file download.
-

Deleting a Template



Note Only user-defined templates can be deleted.

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

Procedure

-
- Step 1** Choose **Configure > Deploy > POAP > POAP Definitions**.
 - Step 2** In the Configuration Steps, click the template hyperlink in the POAP Definitions section.
 - Step 3** Select a template from the list and click **Remove template** icon.
 - Step 4** Click **Yes** to confirm.
-

POAP Template Annotation

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

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

Format of an annotation statement is as follows:

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



Note Each annotation statement is composed of one or more key-values pair.

- The value can be true, false, or a string.
- If the value is a string, it should be double quoted.

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

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

String hostname;

The table displays the supported keys in the annotation statement:

Table 3: Annotation Keys

Key Name	Default Value	Description
DisplayName	Empty String	The value is displayed as a variable label in the template from GUI, on POAP definition screen.
Description	Empty String	Displays the description next or below the template variable field in the template from GUI.
IsManagement	false	The associated variable is of IP Address type. This will be used as the management IP address. DCNM used this IP address to manage the devices.
IsMultiplicity	false	If true, this single value can take multiple values. For example; when it is used with IsManagement annotation, it allows you to type in multiple IP addresses and assign each IP address to a device.
IsSwitchName	false	The associated variable value is used as the device host name.
IsMandatory	true	It marks the field as mandatory if the value is set as ‘true’.
UseDNSReverseLookup	false	This annotation compliments the IsSwitchName annotation. Once they are associated with a variable. The variable is populated with the reverse DNS name, if available during the creation time of the corresponding POAP definition record.
IsHostPort	false	Trunk ports connected to host/servers.
IsVPCDomainID	false	Used as the vPC Domain ID.
IsVPCPeerLinkSrc	false	Used as the VPC IPv4 source address.
IsVPCPeerLinkDst	false	Used as the VPC IPv4 peer address.
IsVPCPeerLinkPortChannel	false	Used for VPC port channel.
IsVPCLinkPort	false	Used for VPC interface.
IsVPC	false	Used as a VPC record.
IsVPCID	false	Individual VPC ID.
IsVPCPortChannel	false	Individual VPC port channel.
IsVPCPort	false	VPC Interface.

POAP Definitions

The POAP switch definition has two major functions:

- Monitoring switch POAP process
- Managing POAP switch configuration

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

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



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

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

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

Fields and Icons	Description
Diff State	<p>Specifies if the configuration defined in POAP is different from the running configuration on the device. If a difference is detected, the user has an option to make changes to the device configuration, thereby ensuring that the configuration on the device is sync with the POAP configuration. The different states are:</p> <ul style="list-style-type: none"> • NA—Specifies that no POAP definition is configured on DCNM for the particular device; therefore, no difference computation can be made. • Diff Detected—Specifies that few configuration differences are detected between POAP definition in DCNM and the running configuration on the switch. You can review the difference statements and choose the commands to deploy to the device, and synchronize the running configuration with the POAP definition. • No Diff Detected—Specifies that there was no configuration diff perceived between POAP definition and the running configuration on the switch. • Error—Specifies that an error has occurred during diff computation. Refer to the logs to troubleshoot the issue.
Model	Specifies the model of the switch.
Template Config File Name	<p>Specifies the template used for creating the POAP definition. Fabric and IPFabric POAP templates are available.</p>
Bootscrip Last Updated Time	Specifies the last updated time for bootscrip.
Last Published	Specifies the last published time for the POAP definition.
POAP Creation Time	Specifies the time when the POAP definition was created.
System Image	Specifies the System Image used while creating the POAP definition.
Kickstart Image	Specifies the kickstart image used the POAP definition.
Icons	
Add	Allows you to add a POAP definition. For more information, see Creating a POAP Definition, on page 12 .

Fields and Icons	Description
Edit	Allows you to edit a POAP definition. For more information, see Editing a POAP Definition, on page 14 .
Delete	Allows you to delete a POAP definition. For more information, see Deleting POAP Definitions, on page 14 .
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 15 .
Change Image	Allows you to change the image for the defined POAP definition. For more information, see Change Image, on page 15 .
Boot Log	Display the list and view log files from the device bootflash.
Update Serial Number	Allows the user to modify the serial number of the POAP definition.
Refresh Switch	Refreshes the list of switches.
Refresh Diff State	Refreshes the Diff state.
Show Filter	Filters list of switches based on the defined value for each column.
Print	Prints the list of devices and their details.
Export	Exports the list of devices and their details to a Microsoft Excel spreadsheet.
Select Columns	Displays the columns to be displayed. You can choose to show/hide a column.



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

This section contains the following:

Creating a POAP Definition

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

Procedure

Step 1

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

- Step 2** From the **Scope** drop-down list, select the scope for POAP definition.
- Step 3** Click **Add** to add a new POAP definition.
- Step 4** Click **Generate Definition** radio button to generate POAP definition from a template, and click **Next** to specify the switch details.
- Step 5** Enter the serial number of switches that are separated by comma. Alternatively, you can click **Import from CSV File** to import the list of switches.
- Note** The serial number cannot be changed after you create the POAP definition. Verify that the serial numbers do not contain spaces, the POAP will not work otherwise.
- Step 6** Use the drop-down list to select the Switch Type.
- Step 7** Use the drop-down list to select the Image Server.
- Step 8** Use the drop-down list to select the System Image and Kickstart image.
- Step 9** Specify the Switch Username and Switch Password.
- Step 10** Click **Next** to Select the Switch Config Template.
- Step 11** Use the drop-down to select the Template and click View to specify the Template Parameters.
- Step 12** Enter Template Parameters.
- Step 13** From the **Settings File** drop-down list to select the file. If the settings file is unavailable, click **Save Parameter** as New Settings File button to specify a name for the settings file.
- Step 14** Select the variables and click **Manage**.
- Step 15** Click **Add** to see the variables to be saved.
Specify a name for the settings file and click **Save**.
- Step 16** Click **Manage** to modify the settings file parameters.
- Step 17** Click **Preview CLI** to view the generated configuration.
- Step 18** Click **Finish** to publish the POAP definition.
- Step 19** Click **Next** to generate the configuration.
-

Uploading a POAP Definition

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

Procedure

- Step 1** Choose **Configure > Deploy > POAP > POAP Definitions**.
- Step 2** Click **Upload Startup Config** radio button to upload startup configuration to the POAP repository Server, and click **Next** to enter the switch details.
- Step 3** Enter the serial number of switches separated by comma.
- Step 4** Use the drop-down to select the Switch Type.
- Step 5** Use the drop-down to select the Image Server.
- Step 6** Use the drop-down to select the System Image and Kickstart Image.
- Step 7** Specify the Switch User Name and Password.
- Step 8** Click **Browse** to select the upload configuration file.

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

Editing a POAP Definition

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

Procedure

- Step 1** Choose **Configure > Deploy > POAP > POAP Definitions**.
- Step 2** Select the POAP switch definitions from the list and click the **Edit** icon.
- Step 3** Follow the steps listed in [Creating a POAP Definition, on page 12](#) and [Uploading a POAP Definition, on page 13](#) sections.
- Note** You can select multiple POAP definitions with similar parameters to edit POAP definition.
-

Deleting POAP Definitions

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

Procedure

- Step 1** Choose **Configure > Deploy > POAP > POAP Definitions**.
- Step 2** Select the POAP switch definitions from the list and click **Delete** icon.
- Step 3** Click **Yes** to delete the switch definitions.
- A prompt appears to delete the device from the data source. Check or uncheck the checkbox based if you want to delete the switches associated with the POAP Definition.
- Step 4** Click **OK** to confirm to delete the device. Based on the check box, the device will be deleted from the data source also.
-

Publishing POAP Definitions

Procedure

- Step 1** Choose **Configure > Deploy > POAP > POAP Definitions**.
- Step 2** Select the POAP switch definitions from the list and click **Publish**.
- Step 3** Click **Yes** to publish the switch definitions.
-

Write, Erase, and Reload the POAP Switch Definition

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

Procedure

- Step 1** Choose **Configure > Deploy > POAP > POAP Definitions**.
- Step 2** Select the POAP switch definitions from the list and click the **Edit** icon.
- Step 3** Click **Write Erase and Reload**.

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

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

Change Image

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

Procedure

- Step 1** Choose **Configure > Deploy > POAP > POAP Definitions**.
- Step 2** Select the POAP switch definitions from the list and click the **Edit** icon.
- Step 3** Select the switch for which you must change the image. Click **Change Image**.

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

The **Multi Device Image Change** window is displayed.

- Step 4** From the **Image Server** drop-down list, select the server where the new image is stored.
 - Step 5** From the **System Image** drop-down list, select the new system image.
 - Step 6** From the **Kickstart Image** drop-down list, select the new image which replaces the old image.
 - Step 7** Click **OK** to apply and change the image.
-

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

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

Procedure

- Step 1** Ensure that the old switch is in place with POAP definition and discovered.
- Step 2** Manually update the serial number in Cisco DCNM on the POAP screen.

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

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

Step 3 Physically remove the old switch from the network.

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

Step 5 Manually rediscover the switches in Cisco DCNM.

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

Cable Plan



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

The Cable plan configuration screen has the following options:

Create a Cable Plan

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

Procedure

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

Step 2 Click **Create Cable Plan**.

In the Create Cable Plan pop-up, use the radio button to select the options.

Step 3 If you select:

- a) **Capture from existing deployment:** You can ascertain the Inter-Switch Links between existing switches that are managed by DCNM and “lock down” the cable plan based on the existing wiring.
- b) **Import Cable Plan File:** You decide how to wire the switches (or how they are already wired) and select an XML file for import into DCNM.

Viewing an Existing Cable Plan Deployment

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

Procedure

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

- Step 2** Click **View**.
 - Step 3** In the **Cable Plan – Existing Deployment** window, you can view the existing cable plan deployments.
 - Step 4** You can use the **Table View** and **XML View** icons to change the view of the cable plan deployments table.
-

Deleting a Cable Plan

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

Procedure

- Step 1** Choose **Configure > Deploy > POAP > Cable Plan**.
 - Step 2** Click **Delete** icon.
 - Step 3** Click **Yes** to confirm deletion.
-

Deploying a Cable Plan

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

Procedure

- Step 1** Choose **Configure > Deploy > POAP > Cable Plan**.
 - Step 2** In the Switches table, use the checkbox to select the cable plan and click **Deploy a Cable Plan**.
 - Step 3** Click **Yes** to confirm deployment.
-

Revoking a Cable Plan

Procedure

- Step 1** Choose **Configure > Deploy > POAP > Cable Plan**.
 - Step 2** In the Switches table, use the check box to select cable plans, and click **Revoke a Cable Plan**.
 - Step 3** Click **Yes** to confirm.
-

Viewing a Deployed Cable Plan from Device

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

Procedure

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

- Step 2** In the Switches table, click **In Sync** or **Out of Sync** hyperlink in the cable plan status column.
- Step 3** You can use the **Table View** and **XML View** icons to change the view of the cable plan table.

Templates

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

Template Library

Template Library includes the following tabs:

Template Library

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

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

Table 4: Templates Operations

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



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

Table 5: Template Properties

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

Table 6: Advanced Template Properties

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

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

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

This section contains the following:

Template Structure

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

This section contains the following:

Template Format

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

Property Name	Description	Valid Values	Optional?
name	The name of the template	Text	No
description	Brief description about the template	Text	Yes
userDefined	Indicates whether the user created the template. Value is 'true' if user created.	"true" or "false"	Yes
supportedPlatforms	List of device platforms supports this configuration template. Specify 'All' to support all platforms.	N1K, N3K, N3500, N4K, N5K, N5500, N5600, N6K, N7K, N9K, MDS, VDC, N9K-9000v, IOS-XE, IOS-XR, Others, All Nexus Switches list separated by comma.	No
templateType	Specifies the type of Template used.	<ul style="list-style-type: none"> • 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?
		<ul style="list-style-type: none"> • CLI <ul style="list-style-type: none"> • N/A • POAP <ul style="list-style-type: none"> • N/A • VXLAN • FABRICPATH • VLAN • PMN • POLICY <ul style="list-style-type: none"> • VLAN • NIERFACE_VLAN • INTERFACE_VPC • NIERFACE_ETHNET • INTERFACE_BD • NIERFACE_FNL • INTERFACE_FC • NIERFACE_MGMT • NIERFACE_LOOBACK • INTERFACE_NVE • INTERFACE_VFC • NIERFACE_NFCNL • DEVICE • FEX • NIERFACE_LINK • NIERFACE_LINK • INTERFACE • SHOW <ul style="list-style-type: none"> • VLAN • NIERFACE_VLAN • INTERFACE_VPC 	

Property Name	Description	Valid Values	Optional?
		<ul style="list-style-type: none"> • INTERFACE_HRNET • INTERFACE_BD • INTERFACE_CHANL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_OOB • INTERFACE_NVE • INTERFACE_VFC • INTERFACE_CHANL • DEVICE • FEX • INTERFACE_FABRIC_LINK • INTERFACE_FABRIC_LINK • INTERFACE • PROFILE <ul style="list-style-type: none"> • VXLAN • FABRIC <ul style="list-style-type: none"> • NA 	

Property Name	Description	Valid Values	Optional?
		<ul style="list-style-type: none">• ABSTRACT<ul style="list-style-type: none">• VLAN• INTERFACE_VLAN• INTERFACE_VPC• INTERFACE_HRNT• INTERFACE_BD• INTERFACE_CHANL• INTERFACE_FC• INTERFACE_MGMT• INTERFACE_COBACK• INTERFACE_NVE• INTERFACE_VFC• INTERFACE_CHANL• DEVICE• FEX• NIRA_FRC_LINK• NIER_FRC_LINK• INTERFACE	

Property Name	Description	Valid Values	Optional?
contentType		<ul style="list-style-type: none"> • CLI <ul style="list-style-type: none"> • TEMPLATE_CLI • POAP <ul style="list-style-type: none"> • TEMPLATE_CLI • POLICY <ul style="list-style-type: none"> • TEMPLATE_CLI • PYTHON • SHOW <ul style="list-style-type: none"> • TEMPLATE_CLI • PROFILE <ul style="list-style-type: none"> • TEMPLATE_CLI • PYTHON • FABRIC <ul style="list-style-type: none"> • PYTHON • ABSTRACT <ul style="list-style-type: none"> • TEMPLATE_CLI • PYTHON 	Yes
implements	Used to implement the abstract template.	Text	Yes
dependencies	Used to select the specific feature of a switch.	Text	Yes
published	Used to Mark the template as read only and avoids changes to it.	“true” or “false”	Yes

Template Variables

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

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

Variable Type	Valid Value	Iterative?
ipAddressWithoutPrefix	Example: 192.168.1.1 or Example: 1:2:3:4:5:6:7:8	No
ipV4Address	IPv4 address	No
ipV4AddressWithSubnet	Example: 192.168.1.1/24	No
ipV6Address	IPv6 address	No
ipV6AddressWithPrefix	Example: 1:2:3:4:5:6:7:8 22	No
ipV6AddressWithSubnet	IPv6 Address with Subnet	No
ISISNetAddress	Example: 49.0001.00a0.c96b.c490.00	No
long	Example: 100	No
macAddress	14 or 17 character length MAC address format	No
string	Free text, for example, used for the description of a variable Example: string scheduledTime { regularExpr="^([01]\d 2[0-3]):([0-5]\d)\$"; }	No
string[]	Example: {a,b,c,str1,str2}	Yes

Variable Type	Valid Value	Iterative?
struct	<p>Set of parameters that are bundled under a single variable.</p> <pre> struct <structure name declaration > { <parameter type> <parameter 1>; <parameter type> <parameter 2>; } [<structure_inst1>] [, <structure_inst2>] [, <structure_array_inst3 []>; struct interface_detail { string inf_name; string inf_description; ipAddress inf_host; enum duplex { validValues = auto, full, half; }; }myInterface, myInterfaceArray[]; </pre>	<p>No</p> <p>Note If the struct variable is declared as an array, the variable is iterative.</p>
wwn (Available only in Cisco DCNM Web Client)	<p>Example: 20:01:00:08:02:11:05:03</p>	No

Variable Meta Property

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

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

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

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

Variable Type	Description	Variable Meta Property											
		default Value	valid Values	decimal Length	min	max	min Slot	max Slot	min Port	max Port	min Length	max Length	regular Expr
ipAddressList	<p>You can have a list of IPv4, IPv6, or a combination of both types of addresses.</p> <p>Example 1:</p> <p>122.3.9, 122.3.9, 122.3.15, 122.3.10</p> <p>Example 2:</p> <p>0:0:0:0:0:0:0:0, 0:0:0:0:0:0:0:0, 0:0:0:0:0:0:0:0</p> <p>Example 3:</p> <p>122.3.9, 122.3.9, 0:0:0:0:0:0:0:0, 122.3.24</p> <p>Note</p> <p>Separate the addresses in the list using commas and not hyphens.</p>	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
ipAddr	IPv4 or IPv6 Address (does not require prefix)												
ipAddr	IPv4 address	Yes											
ipAddr	IPv4 Address with Subnet	Yes											
ipAddr	IPv6 address	Yes											
ipAddr	IPv6 Address with prefix	Yes											
ipAddr	IPv6 Address with Subnet	Yes											
ipAddr	Example: 10.1.1.1/24												
long	Example: 100	Yes			Yes	Yes							
macAddr	MAC address												

Variable Type	Description	Variable Meta Property											
		default Value	valid Values	decimal Length	min	max	min Slot	max Slot	min Port	max Port	min Length	max Length	regular Expr
struct	Set of parameters that are bundled under a single variable. struct <structure name declaration> { <parameter type> <parameter 1>; <parameter type> <parameter 2>; } [<struct1>, <struct2>, [,<struct3>] []>;												
wwn	WWN address												

Example: Meta Property Usage

```
##template variables

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

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

struct interface_a{
```

```

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

##

```

Variable Annotation

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



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

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

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

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

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

Example: AutoPopulate Annotation

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

Example: DisplayName Annotation

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

Example: IsMandatory Annotation

```
##template variables
@(IsMandatory="ipv6!=null")
IPv4Address ipv4;
@(IsMandatory="ipv4!=null")
IPv6Address ipv6;
##
```

Example: IsMultiLineString Annotation

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

IsShow Annotation

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

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

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

Example: Warning Annotation

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

Templates Content

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



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

Template content is governed by the usage of variables.

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

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

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

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

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

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

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

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

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

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

```
Syntax: if(<operand 1> <logical operator> <operand 2>){
command1 ..
command2..
..
}
else if (<operand 3> <logical operator> <operand 4> )
{
Command3 ..
Command4..
..
}
else
{
Command5 ..
Command6..
..
}
Example: if-else if-else statement
if($$USER_NAME$$ == 'admin'){
Interface2/10
no shut
}
else {
Interface2/10
shut
}
```

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

```
Syntax:
foreach <loop index variable> in $$<loop variable>$$ {
@<loop index variable> ..
}
Example: foreach Statement
foreach ports in $$MY_INF_RANGE$${
interface @ports
```

```
no shut
}
```

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

In the variable section, you can include the following command:

- **@(IsMandatory=false)**
- **Integer frequency;**

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

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

Template Content Editor

The template content editor has the following features:

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

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

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

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

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

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

Template Editor Settings

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

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

Advanced Features

The following are the advanced features available to configure templates.

- **Assignment Operation**

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

Assignment operation can be used under the following guidelines:

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

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

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

- **Evaluate methods**

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

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

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

```
Example1:
$$somevar$$ = evalscript(add, "100", $$anothervar$$)
```

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

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

You can call a method that is located at the backend of the Java script file.

- Dynamic decision

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



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

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

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

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

- Template referencing

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

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

```
##
##template content
vlan $$vlan_id$$
##

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

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

- Solution POAP Templates for VXLAN and FabricPath

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

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

Adding a Template

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

Procedure

-
- Step 1** Choose **Configure > Templates > Template Library > Templates**.
- The **Templates** window is displayed with the name of the template along with its description, supported platforms, and tags.
- Step 2** Click **Add** to add a new template.
- The Template Properties window appears.
- Step 3** Specify a template name, description, tags, and supported platforms for the new template.
- Step 4** Specify a **Template Type** for the template. Select **POAP** to make this template available when you power on the application.
- Note** The template is considered as a CLI template if **POAP** is not selected.
- Step 5** Select a **Template Sub Type** and **Template Content Type** for the template.

- Step 6** Click the **Advanced** tab to edit other properties like **Implements**, **Dependencies**, **Published**, and **Imports**. Select **Published** to make the template read-only. You cannot edit a published template.
- Step 7** From the **Imports > Template Name** list, check the template check box.
- The base template content is displayed in the **Template Content** window. The base template displays the template properties, template variables, and template content. This template can be imported in to another template and the base template content is substituted in the appropriate place of the extending template. When you launch the extended template, the parameter inputs for the base template are also obtained. Also, the substituted content is used for complete CLI command generation.
- Note** The base templates are CLI templates.
- Step 8** Click **OK** to save the template properties, or click the cancel icon at the top-right corner of the window to revert the changes.
- Note** You can edit the template properties by clicking **Template Property**.
- Step 9** Click **Template Content** to edit the template syntax. For information about the structure of the Configuration Template, see the *Template Structure* section.
- Step 10** Click **Validate Template Syntax** to validate the template values.
- If an error or a warning message appears, you can check the validation details in **Validation Table** by clicking the error and warnings field.
- Note** You can continue to save the template if there are warnings only. However, if there is an error, you must edit the templates to fix the errors before you proceed. Click the line number under the Start Line column to locate the error in the template content. You will get an error if you validate a template that does not have a template name.
- Step 11** Click **Save** to save the template.
- Step 12** Click **Save and Exit** to save the configuration and go back to the configuring templates screen.

Configuring Template Job

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

Procedure

- Step 1** Choose **Configure > Templates > Template Library > Templates**.
- Step 2** Select a template.
- Note** Config Job wizard is applicable only for CLI templates.
- Step 3** Click **Launch job creation wizard** icon and click **Next**.
- Step 4** Use the drop-down to select **Device Scope**.
- The devices that are configured under the selected **Device Scope** are displayed.
- Note** If no devices are displayed, check if the device LAN credentials are configured by choosing **Administration > Credentials Management > LAN Credentials**.

- Step 5** Use the arrows to move the devices to the right column for job creation and click **Next**.
- Step 6** In the **Define Variable** section, specify the VSAN_ID, VLAN_ID, ETH_SLOT_NUMBER, VFC_SLOT_NUMBER, SWITCH_PORT_MODE, ETH_PORT_RANGE and ALLOWED_VLANS values.
- Note** Based on the selected template, variables vary.
- Step 7** In the **Edit Variable Per Device** section, double click the fields to edit the variables for specific devices and click **Next**.
- Step 8** If you have selected multiple devices, use the drop-down to select a specific device and preview its configuration. Click **Back** to edit the configuration or click **Next**.
- Step 9** Specify a job name and description.
- The Device Credentials are populated from **Administration > Credentials Management > LAN Credentials**.
- Step 10** Use the radio button to select **Instant Job** or **Schedule Job**.
- If you select **Schedule Job**, specify the date and time for the job delivery.
- Step 11** Use the check box to select **Copy Run to Start**.
- Step 12** If you want to configure more transaction and delivery options, use the check box to select **Show more options**.
- Step 13** Under **Transaction Options(Optional)**, if you have a device with rollback feature support, select **Enable Rollback** check box and select the appropriate radio button.
- You can choose one of the following options by selecting the appropriate radio button:
- **Rollback the configuration on a device if there is any failure on that device**
 - **Rollback the configuration on all the devices if there is any failure on any device**
 - **Rollback the configuration on a device if there is any failure on any device and stop further configuration delivery to remaining devices**
- Step 14** Under **Delivery Options (Optional)**, specify the command response timeout in seconds and use the radio button to select a delivery order. The value of command response timeout ranges from 1 to 180.
- You can choose one of the following options by selecting the appropriate radio button:
- **Deliver configuration one device at a time in sequential**
 - **Delivery configuration in parallel to all devices at the same time**
- Step 15** Click **Finish** to create the job.
- A confirmation message is displayed that the job has been successfully created. The jobs are listed in the **Jobs** window.
-

Modifying a Template

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

Procedure

- Step 1** From **Configure > Templates > Template Library > Templates**, select a template.
- Step 2** Click **Modify/View template**.
- Step 3** Edit the template description and tags.
The edited template content is displayed in a pane on the right.
- Step 4** From the **Imports > Template Name** list, check the template check box.
The base template content is displayed in the **Template Content** window. You can edit the template content based on your requirement in the **Template Content** window. Click the help icon next to the **Template Content** window for information about editing the content of the template.
- Step 5** Edit the supported platforms for the template.
- Step 6** Click **Validate Template Syntax** to validate the template values.
- Step 7** Click **Save** to save the template.
- Step 8** Click **Save and Exit** to save the configuration and go back to the configuring templates screen.
-

Copying a Template

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

Procedure

- Step 1** Choose **Configure > Templates > Template Library > Templates**, and select a template.
- Step 2** Click **Save Template As**.
- Step 3** Edit the template name, description, tags, and other parameters.
The edited template content is displayed in the right-hand pane.
- Step 4** From the **Imports > Template Name** list, check the template check box.
The base template content is displayed in the **Template Content** window. You can edit the template content that is based on your requirement in the **Template Content** window. Click the help icon next to the **Template Content** window for information about editing the content of the template.
- Step 5** Edit the supported platforms for the template.
- Step 6** Click **Validate Template Syntax** to validate the template values.
- Step 7** Click **Save** to save the template.
- Step 8** Click **Save and Exit** to save the configuration and go back to the configuring templates screen.
-

Deleting a Template

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

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

Procedure

- Step 1** Choose **Configure > Templates > Template Library > Templates**.
- Step 2** Use the check box to select a template and click **Remove template** icon.
- The template is deleted without any warning message.
-

What to do next

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

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

Importing a Template

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

Procedure

- Step 1** Choose **Configure > Templates > Template Library > Templates** and click **Import Template**.
- Step 2** Browse and select the template that is saved on your computer.
- You can edit the template parameters, if necessary. For information, see [Modifying a Template, on page 44](#).
- Note** The “\n” in the template is considered as a new line character when imported and edited, but it works fine when imported as a ZIP file.
- Step 3** Click **Validate Template Syntax** to validate the template.
- Step 4** Click **Save** to save the template or **Save and Exit** to save the template and exit.
- Note** You can import Cisco-defined FabricPath and IP VXLAN Programmable Fabric POAP Templates to the Cisco DCNM Web Client. For more information, see *Installing POAP Templates*.
-

Exporting a Template

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

Procedure

- Step 1** Choose **Configure > Templates > Template Library > Templates**.
- Step 2** Use the check box to select a template and click **Export Template**.

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

Installing POAP Templates

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

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

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

Procedure

- Step 1** Navigate to <https://software.cisco.com/download/release.html>, and download the file.
You can choose one of the following:
- `dcnm_ip_vxlan_fabric_templates.10.0.1a.zip`
 - `dcnm_fabricpath_fabric_templates.10.0.1a.zip` file
- Step 2** Unzip and extract the files to the local directory on your computer.
- Step 3** Choose **Configure > Templates > Template Library > Templates**.
- Step 4** Click **Import Template**.
- Step 5** Browse and select the template that is saved on your computer. You can edit the template parameters, if necessary.
- Step 6** Check **POAP** and **Publish** check box to designate these templates as POAP templates.
- Step 7** Click **Validate Template Syntax** to validate the template.
- Step 8** Click **Save** to save the template or **Save and Exit** to save the template and exit.
-

Configuring Jobs

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

Procedure

- Step 1** Choose **Configure > Templates > Templates Library > Jobs**.
The jobs are listed along with the Job ID, description and status. The latest task will be listed at the top.
- Note** If failover is triggered in Native HA, the Job ID sequence number is incremented by 32.
- Step 2** Click **Show Filter** to filter the list.
In the **Status** column, use the drop-down to select the job status.

Step 3 Select a job and click the **Delete** icon to delete the job.

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

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

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

Backup

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

Switch Configuration

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

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

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

Table 7: 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 8: Switch Configuration Field and Description

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

This section contains the following:

Copy Configuration

You can copy the configuration files to the same device, to another device, or multiple devices concurrently. Perform the following task to view the status of tasks.

Procedure

-
- Step 1** From Cisco DCNM home page, choose **Configure > Backup > Switch Configuration**. Select any startup/running/archive configuration of the device that you must copy.
- Step 2** Click **Copy Configuration to bootflash**.
Copy Configuration to bootflash page appears, displaying the **Source Configuration Preview** and **Selected Devices** area.
Source Configuration Preview area shows the contents of running/startup/version configuration file which is copied to the devices.
- Step 3** In the **Selected Devices** area, check the device name check box to copy the configuration to the device.
- Note** You can select multiple destination devices to copy the configuration.

The selected devices area shows the following fields:

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

- Step 4** Click **Copy**.
A confirmation window appears.
- Step 5** Click **Yes** to copy the configuration to the destination device configuration.
-

View Configuration

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

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

Procedure

- Step 1** From Cisco DCNM home page, choose **Configure > Backup > Switch Configuration**. Click the arrow next to the device name to view the configuration files on the device. Select the configuration file radio button to view the configuration file.
- Step 2** Click the View Configuration.
- The View Configuration window appears showing the configuration file content.
-

Delete Configuration

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



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

Procedure

- Step 1** From Cisco DCNM home page, choose **Configure > Backup > Switch Configuration**. Click the arrow next to the device name to view the configuration files on the device.
- Step 2** Click the configuration file radio button to be deleted.
- Note** You can delete multiple configuration files. However, you cannot delete startup, or running configuration files.
- Step 3** Click **Yes** to delete the configuration file.
-

Compare Configuration Files

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

Perform the following task to compare the configuration files.

Procedure

- Step 1** Navigate to **Configure > Backup > Switch Configuration**. Click the arrow next to the device name to view the configuration files on the device.
- Step 2** Check the check box and select two configuration files to compare.
- The first file that you selected is designated as Source and the second configuration file is designated as the Target file.
- Step 3** Click **Compare Configuration**.
- View Config Diff** page appears, displaying the difference between the two configuration files.
- The Source and Target configuration files content is displayed in two columns. From the drop-down list in the right-top corner, choose **All** to view the entire configuration. You can also choose **Changed** to view the configuration differences of the configuration files.
- The differences in the configuration file are shown in the table, with legends.
- **Red**: Deleted configuration details.
 - **Green**: New added configuration.
 - **Blue**: Modified configuration details.
- Step 4** Click **Copy to Target** to copy the source configuration to the target configuration file. Click **Cancel** to revert to the configuration details page.
- The Copy Configuration window displays the source configuration preview and the target device of the destination configuration. The selected devices area shows the following fields:
- Device Name—Specifies the target device name to which the source configuration is copied.
 - IP Address—Specifies the IP Address of the destination device.
 - Group—Specifies the group to which the device belongs.
 - Status—Specifies the status of the device.
- Step 5** Click **Yes** to copy the configuration to the destination device configuration.
-

Export Configuration

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

Procedure

- Step 1** From Cisco DCNM home page, choose **Configure > Backup**, select a configuration to export.
- Step 2** Click **Export Configuration**.

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

Import Configuration File

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

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

Procedure

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

The file server directory opens.

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

A confirmation screen appears.

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

The file name can be alphanumeric. It can also have a period (.), underscore (_), and a space. You can import only files with the .cfg extension.

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

The imported configuration file appears as a User Imported file.

Restore Configuration

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



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

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

Procedure

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

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

Note

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

Step 3

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

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

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

Note

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

Archive Jobs

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

**Note**

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

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

Field	Description
User	Specifies who created this job.
Group	Specifies the group to which this job belongs.
Group Job	Specifies whether it is a group job or a per-device job. The values are true or false .
Schedule	Specifies the schedule of the job. Also show the recurrence information.
Last Execution	Specifies the date and time at which this job was last executed.
Job Status	Specifies if the job was successful, scheduled, running, or failure.

Field	Description
	Note Running and Scheduled status is not applicable for existing jobs in an upgraded Cisco DCNM.
User Comments	Specifies the comments or description provided by the user.

Archive Jobs

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



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

Procedure

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

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

A backup is scheduled as defined.

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

Note You can schedule a job to run **Now** even if a job is already scheduled.
 - **Daily:** Check the check box on the days you want this job to be executed. The time at which this job will be executed is determined by the **Start At** field.
 - **Real Time:** Configure the job to be executed if there is any configuration changes in the device. The device must be quiet for 5 minutes, after which the DCNM Sever will execute this job.
 - **Repeat Interval:** Check the Repeat Interval check box to repeat the job at scheduled intervals. Configure the intervals using either days or hours drop-down list.
 - **Comments:** Enter your comments, if any.
- b) In the **Device Selection** area, use the radio button to choose one of the following:
 - **Device Group:** Click the Device Group radio button to select the entire group of devices for this job.

Select the Device Group from the drop-down list.

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

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

Select the devices from the drop-down list.

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

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

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

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

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

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

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

Step 2 To delete a job, from the Cisco DCNM home page, choose **Configure > Backup > Switch Configuration > Archive Jobs > Archive Jobs**, and select a job.

- a) Click **Delete Job**.

The Schedule, Device Selection and the Selected devices for this job is displayed.

- b) Click **Delete**.

Step 3 To view the details of the job, from the Cisco DCNM home page, choose **Configure > Backup > Switch Configuration > Archive Jobs > Archive Jobs**, and check the job check box.

- a) Click **View/Modify Job**.

The Schedule, Device Selection and the Selected devices for this job is displayed.

- b) Modify the required details. Click **OK** to revert to view the list of jobs.

Note

- You cannot modify a job that is scheduled to be run **Now** to one that is scheduled to be run **Daily**.
- You cannot modify the repeat interval duration for an archive job. When you try to modify, the operation fails and the job is deleted. You must delete existing repeat interval archive job and create a new job.

What to do next

You can also configure the Cisco DCNM to retain the number of archived files per device. Choose **Administration > DCNM Server > Server Properties**, and update the **archived.versions.limit** field.

Job Execution Details

The Cisco DCNM **Web Client > Configure > Backup > Switch Configuration > Archive Jobs > Archive Jobs > Job Execution Details** tab shows the following tabs in the Job Execution History table.

Field	Description
Job Name	Displays the system-generated job name.
User	Specifies the persona of the person who created the job.
Device Group	Specifies fabric or the LAN group under which the job was created.
Device	Specifies the IP Address of the Device.
Server	Specifies the IP Address of the DCNM Server to which the device is associated with.
Protocol	Specifies if the SFTP, TFTP, or SCP protocol is applied.
Execution time	Specifies the time at which the job was last executed.
Status	Specifies the status of the job. <ul style="list-style-type: none"> • Skipped • Failed • Successful
Error Cause	Specifies the error if the job has failed. The categories are as follows: <ul style="list-style-type: none"> • No change in the configuration. • Switch is not managed by this server. <p>Note If the error cause column is empty, it implies that the job was executed successfully.</p> <p>Hover over the error cause to view the complete description.</p>

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 9: Archive Operations

Icon	Description
Compare	Allows you to compare two configuration files either from different devices or on the same device.
View	Allows you to view a configuration file.

Table 10: Archive Field and Description

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

This section contains the following:

Compare Configuration Files

You can compare one version of a configuration file with another version of the same configuration file in the same device, or the configuration files of two different devices.

To compare the configuration files from the Cisco DCNM Web UI, perform the following steps:

Procedure

-
- Step 1** Choose **Configure > Backup > Archives**.
- Step 2** In the **Archives** area, click the arrow that is adjacent the name of the device whose configuration files you want to view. The list of configuration files is displayed.

- Step 3** Check the check box next to configuration files and select two configuration files to compare.
- The first file that you select is designated as the source and the second configuration file is designated as the target file.
- Step 4** Click **Compare**.
- The **View Config Diff** page displays the difference between the two configuration files.
- The Source and Target configuration files content are displayed in two columns. Choose **All** from the drop-down list in the right-top corner to view the entire configuration. Choose **Changed** to view the configuration differences between the configuration files.
- The differences in the configuration files are shown in a table, with legends.
- **Red**: Deleted configuration details.
 - **Green**: New added configuration.
 - **Blue**: Modified configuration details.
-

View Configuration

You can view an archived configuration file.

To view or edit the configuration file for the devices from the Cisco DCNM Web UI, perform the following steps:

Procedure

- Step 1** Choose **Configure > Backup > Archives**.
- The **Archives** window is displayed.
- Step 2** Click the arrow that is next to the name of the device whose configuration files you want to view.
- The list of configuration files are displayed.
- Step 3** Select the radio button that is next to the corresponding file you want to view.
- Step 4** Click the **View** configuration icon.
- The **View** configuration window appears showing the configuration file content in the right column.
-

Network Config Audit

Cisco DCNM provides auditing for the configuration changes across the network switches. The Network Audit Reporting feature enables you to generate audit report so that you can track the added, deleted, or modified configurations. You will be able to generate the network audit reports only when you have existing archival jobs. Using the generated reports, you can view the config differences on a device for a specified period.

This section contains the following:

Generating Network Config Audit Reports

To generate the network config audit reports from the Cisco DCNM Web UI, perform the following steps:

Procedure

- Step 1** Choose **Configure > Backup > Network Config Audit**.
The **Network Audit Report** window is displayed.
- Step 2** In the **Devices** drop-down list, choose the devices to generate a report.
- Step 3** Specify the **Start Date** and the **End Date**.
- Step 4** Click **Generate Report** to view the configuration differences. The configuration differences are color-coded.
- Red: Deleted Configuration
 - Green: Newly Added Configuration
 - Blue: Changed configuration
 - Strikethrough: Old configuration

After you generate a report, you can export the configuration reports into an HTML file.

Creating a Network Config Audit Report

To create a network config audit job and view the configuration differences between the devices from the Cisco DCNM Web UI, perform the following steps:

Procedure

- Step 1** Choose **Monitor > Report > Generate**.
The left pane shows various reports that you can create.
- Step 2** Choose **Common > Network Config Audit**.
- Step 3** In the **Report Name** field, enter the name of the report.
- Step 4** In the **Repeat** field, choose the appropriate repeat interval, that is, Daily, Weekly, or Monthly.
Daily job generates a report of configuration differences for all the selected devices for last 1 day. Weekly job generates a report for the last 7 days, and the monthly job generates a report for the last 30 days.
- Step 5** In the **Start** and **End** date fields, specify the start and end date for the report.
- Step 6** In the **Email Report** field, specify the email delivery options.
- No: Select this option if you do not want to send the report through email.
 - Link Only: Select this option if you want to send the link to the report.
 - Contents: Select this option if you want to send the report content.

If you select Link Only or the Contents option, enter the email address and subject in the **To** and **Subject** fields.

Monitoring Network Config Audit Report

To monitor the network config audit report from the Cisco DCNM Web UI, perform the following steps:

Procedure

- Step 1** Choose **Monitor > Report > View**.
- Step 2** Choose **Common > Network Config Audit** in the left pane to the network config audit reports.

Deleting a Network Config Audit Report

To delete a network config audit report from the Cisco DCNM Web UI, perform the following steps:

Procedure

- Step 1** Choose **Monitor > Report > View**.
- Step 2** Choose **Common > Network Config Audit**.
The **View Reports** window is displayed with the reports that you have created.
- Step 3** Select the reports that you want to delete, and click the **Delete** icon.

Image Management

Upgrading your devices to the latest software version manually might take a long time and prone to error, which requires a separate maintenance window. To ensure rapid and reliable software upgrades, image management automates the steps associated with upgrade planning, scheduling, downloading, and monitoring. Image management is supported only for Cisco Nexus switches.



Note Before you upgrade, ensure that the POAP boot mode is disabled for Cisco Nexus 9000 Series switches and Cisco Nexus 3000 Series switches. To disable POAP, run the `no boot poap enable` command on the switch console. You can however, enable it after the upgrade.

The **Image Management** menu includes the following submenu:

Upgrade [ISSU]

The **Upgrade [ISSU]** menu includes the following submenus:

Upgrade History [ISSU]

This feature enables you to upgrade the Cisco Nexus Platform Switches using In-Service Software Upgrade (ISSU). This upgrade procedure may be disruptive or non-disruptive based on the device configuration. You can select the Kickstart, System, or SSI images required for the upgrade from a remote server using SFTP, SCP, TFTP, FTP or from image repository or the file system on the device. Image repository can use SCP, SFTP, FTP, or TFTP as file transfer protocol. To select the images from the repository, the same needs to be uploaded from **Configure > Image Management > Repositories** tab.

The following table describes the fields that appear on **Configure > Image Management > Upgrade [ISSU] > Upgrade History**.

Field	Description
Task Id	Specifies the serial number of the task. The latest task will be listed in the top. Note If Failover is triggered in Native HA, the Task Id sequence number is incremented by 32.
Task Type	Specifies the type of task. <ul style="list-style-type: none">• 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. <ul style="list-style-type: none">• Planned• In Progress• Completed• Completed with Exceptions Note If the job fails on a single or multiple devices, the status field shows COMPLETED WITH EXCEPTION indicating a failure.
Created Time	Specifies the time when the task was created.
Scheduled At	Specifies the time when the task is specified to be executed. You can also choose to schedule a task to be executed at a later time.
Completed Time	Specifies the time when the task was completed.
Comment	Shows any comments that the Owner has added while performing the task.



Note After a fresh Cisco DCNM installation, this page will have no entries.

You can perform the following:

New Installation

To upgrade the devices that are discovered from the Cisco DCNM, perform the following steps:

Procedure

Step 1 Choose **Configure > Image Management > Upgrade [ISSU] > Upgrade History**.

Step 2 Choose **New Installation** to install, or upgrade the kickstart and the system images on the devices.
The devices with default VDCs are displayed in the **Select Switches** window.

Step 3 Select the check box to the left of the switch name.

You can select more than one switch and move the switches to the right column.

Step 4 Click **Add** or **Remove** icons to include the appropriate switches for upgrade.

The selected switches appear in a column on the right.

Step 5 Click **Next**.

The **Specify Software Images** window appears. This tab displays the switches that you selected in the previous screen. You can choose the images for upgrade as well.

- The **Auto File Selection** check box enables you to specify a file server, an image version, and a path where you can apply the upgraded image to the selected devices.
- In the **Select File Server** drop-down list, select the one of the file servers that is created in the Cisco DCNM repositories.
- In the **Image Version** field, specify the image version. For example, enter 7.3.9.D1.1 in the **Image Version** field if you have selected m9700-sf3ek9-kickstart-mz.7.3.0.D1.1.bin as the image version.
- In the **Path** field, specify the image path. Specify an absolute path if you choose SCP or SFTP. For example, `//root/images/`. Specify a relative path to the FTP or TFTP home directory if you choose FTP or TFTP. Specify the absolute path of the image if you're using TFTP server that is provided by Cisco DCNM, local DCNM TFTP. You can't use the same DCNM TFTP server for creating another job when the current job is in progress.

Step 6 Click **Select Image** in the **Kickstart image** column.

The **Software Image Browser** dialog box appears.

- Note**
- Cisco Nexus 3000 Series and 9000 Series Switches require only the system image to load the Cisco NX-OS operating system. Therefore, the option to select kickstart images for these devices is disabled.
 - If there's an issue in viewing the **Software Image Browser** dialog box, reduce the font size of your browser and retry.

- Step 7** Click **Select Image** in the **System Image** column.
- The **Software Image Browser** dialog box appears.
- Step 8** On the **Software Image Browser** dialog box, you can choose the image from **File Server** or **Switch File System**.
- If you choose **File Server**:
- From the **Select the File server** list, choose the appropriate file server on which the image is stored.
- The servers at **Configure > Image Management > Repositories** are displayed in the drop-down list.
- From the **Select Image** list, choose the appropriate image. Check the check box to use the same image for all other selected devices of the same platform.
- Example: For platform types N7K-C7009 and N7K-C7010, logic matches platform (N7K) and three characters (C70) from subplatform. The same logic is used across all platform switches.
- Note** Only files with BIN extension are listed if you select **File Server**. To view other files, choose **Administration > DCNM Server > Server Properties**, set **FILE_SELECTION_FILTER** to **false**, and restart the server. It is set to **true** by default.
- Click **OK**.
- If the file server selected is either `ftp` or `tftp`, in the text box, enter the relative path of the file from the home directory.
- If you choose **Switch File System**:
- From the **Select Image** list, choose the appropriate image that is located on the flash memory of the device.
- Note** Only files with BIN extension are listed if you select **Switch File System**. To view other files, choose **Administration > DCNM Server > Server Properties**, set **FILE_SELECTION_FILTER** to **false**, and restart the server. It is set to **true** by default.
- Click **OK** to choose the kickstart image or **Cancel** to revert to the **Specify Software Images** dialog box.
- Step 9** The **Vrf** column indicates the name of the virtual routing and forwarding (VRF).
- Step 10** In the **Available Space** column, specify the available space for the **Primary Supervisor** and **Secondary Supervisor** modules of the switch.
- Available Space** column shows the available memory in MB on the switch (for less than 1 MB, it's shown and marked as KB).
- Bootflash browser shows the filename, size, and last modified date for all the files and directories on the switch bootflash. You can delete files by selecting them and clicking **Delete** to increase the available space on the switch.
- Step 11** **Selected Files Size** column shows the size of images that are selected from the SCP or SFTP server.
- If the total size of selected images is greater than available space on a switch, the file size is marked in red. We recommend that you create more space on the switch to copy images to it and install.
- Step 12** Drag and drop the switches to reorder the upgrade task sequence.
- Step 13** Select **Skip Version Compatibility** if you are sure that the version of the Cisco NX-OS software on your device is compatible with the upgraded images that you have selected.
- Step 14** Select **Select Parallel Line Card upgrade** to upgrade all the line cards at the same time.

Upgrading a parallel line card isn't applicable for Cisco MDS devices.

Step 15 Click **Options** under the **Upgrade Options** column to choose the type of upgrade.

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

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

NA is the default value.

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

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

When **NA** is selected under **Upgrade Option 1**, **Upgrade Option 2** is disabled.

When you choose **bios-force** under **Upgrade Option 1**, **Upgrade Option 2** is disabled.

When **non-disruptive** is selected under **Upgrade Option 1**, you can choose **NA** or **bios-force** under **Upgrade Option 2**.

Check the **Use this Option for all other selected devices** check box to use the selected option for all the selected devices and click **OK**.

- Note**
- The upgrade options are applicable only for Cisco Nexus 3000 Series and 9000 Series switches.
 - Selecting the **non-disruptive** option for upgrading does not ensure a non-disruptive upgrade. Perform a compatibility check to ensure that the device supports non-disruptive upgrade.

Step 16 Click **Next**.

If you didn't select **Skip Version Compatibility**, the Cisco DCNM performs a compatibility check.

You can choose to wait until the check is complete or click **Finish Installation Later**.

The installation wizard is closed and a compatibility task is created in **Configure > Image Management > Upgrade [ISSU] > Upgrade History** tasks.

The time that is taken to check the image compatibility depends on the configuration and the load on the device.

The **Version Compatibility Verification** status column displays the status of verification.

If you skip the version compatibility check by choosing **Skip Version Compatibility**, Cisco DCNM displays only the name of the device. The **Current Action** column displays **Completed**, and the **Version Compatibility Verification** column displays **Skipped**.

Step 17 Click **Finish Installation Later** to perform the upgrade later.

Step 18 Click **Next**.

Step 19 Check the **Next** check box to put a device in maintenance mode before upgrade.

Step 20 Check the check box to save the running configuration to the startup configuration before upgrading the device.

- Step 21** You can schedule the upgrade process to occur immediately or later.
- Select **Deploy Now** to upgrade the device immediately.
 - Select **Choose time to Deploy** and specify the time in MMM/DD/YYYY HH:MM:SS format to perform the upgrade later.
This value is relative to the server time. If the selected time to deploy is in the past, the job is executed immediately.
- Step 22** You can choose the execution mode based on the devices and the line cards you have chosen to upgrade.
- Select **Sequential** to upgrade the devices in the order you chose them.
 - Select **Concurrent** to upgrade all the devices at the same time.
- Step 23** Click **Finish** to begin the upgrade process.
The Installation wizard closes and a task to upgrade is created on the **Configure > Image Management > Upgrade [ISSU] > Upgrade History** page.

What to do next

After you complete the ISSU on the switch, ensure that you wait for 20 minutes to allow the switch to reboot, and stabilize the SNMP agent. DCMN discovers polling cycles in order to display the new version of the switch on the Cisco DCMN Web UI.

Finish Installation

You can choose to complete the installation for tasks which was completed on the **Compatibility Check** page. Perform the following task to complete the upgrade process on the devices.

Procedure

- Step 1** Choose **Configure > Image Management > Upgrade [ISSU] > Upgrade History**, select a task for which the compatibility check is complete.
Select only one task at a time.
- Step 2** Click **Finish Installation**.
Software Installation Wizard appears.
- Step 3** Check the check box to save the running configuration to the startup configuration before upgrading the device.
- Step 4** Check the check box to put a device in maintenance mode before upgrade. This option is valid only for the devices that support maintenance mode.
- Step 5** You can schedule the upgrade process to occur immediately or later.
- Select **Deploy Now** to upgrade the device immediately.
 - Select **Choose time to Deploy** and specify the time in DD/MM/YYYY HH:MM:SS format to perform the upgrade later.

- Step 6** You can choose the execution mode that is based on the devices and the line cards that you have chosen to upgrade.
- Select **Sequential** to upgrade the devices in the order in which they were chosen.
 - Select **Concurrent** to upgrade the devices at the same time.

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

View

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

Procedure

- Step 1** Choose **Configure > Image Management > Upgrade [ISSU] > Upgrade History**, check the task ID check box.
- Select only one task at a time.
- Step 2** Click **View**.
- The **Installation Task Details** window appears.
- Step 3** Click **Settings**. Expand the **Columns** menu and choose the details you want to view.
- You can view the following information in this window:
- Location of the kickstart and system images
 - Compatibility check status
 - Installation status
 - Descriptions
 - Logs
- Step 4** Select the device.
- The detailed status of the task appears. For the completed tasks, the response from the device appears.
- If the upgrade task is in progress, a live log of the installation process appears.
- Note**
- This table autorefreshes every 30 secs for jobs in progress, when you're on this window.
 - The switch-level status for an ongoing upgrade on a Cisco MDS switch doesn't appear for other users without SAN credentials. To apply SAN Credentials, choose **Administration > Credentials Management > SAN Credentials**.
-

Delete

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

Procedure

- Step 1** Choose **Configure > Image Management > Upgrade [ISSU] > Upgrade History**, and check the **Task ID** check box.
- Step 2** Click **Delete**.
- Step 3** Click **OK** to confirm deletion of the job.

Switch Level History

You can view the history of the upgrade process at a switch level. You can view the current version of the switch and other details.

The following table describes the fields that appear on **Configure > Image Management > Upgrade [ISSU] > Switch Level History**.

Field	Description
Switch Name	Specifies the name of the switch
IP Address	Specifies the IP Address of the switch
Platform	Specifies the Cisco Nexus switch platform
Current Version	Specifies the current version on the switch software

Click the radio button next to a switch name to select the switch and view its upgrade history. Click **View** to view the upgrade task history for the selected switch.

The following table describes the fields that appear on **Configure > Image Management > Upgrade [ISSU] > Switch Level History > View Device Upgrade Tasks**:

Field	Description
Owner	Specifies the owner who initiated the upgrade.
Job Status	Specifies the status of the job. <ul style="list-style-type: none"> Planned In Progress Completed
KickStart Image	Specifies the kickStart image that is used to upgrade the Switch.
System Image	Specifies the system image that is used to upgrade the switch.
Completed Time	Specifies the date and time at which the upgrade was successfully completed.
Status Description	Specifies the installation log information of the job.

Patch [SMU]

The Patch [SMU] menu includes the following submenus:

Installation History

This feature allows you to activate or deactivate packages using Software Maintenance Update (SMU). Personnel with Admin privileges can perform this operation.

The following table describes the fields that appear on **Configure > Image Management > Patch [SMU] > Installation History**.

Field	Description
Task Id	Specifies the serial number of the task. The latest task is listed at the top. The tasks are performed in the sequential order.
Switch Name	Specifies the name of the switch for which the patch file is installed.
IP Address	Specifies the IP Address of the device.
Task	Specifies if the patch is installed or uninstalled on this device.
Package	Specifies the name of the patch file.
Status	Specifies the status of installation or uninstallation of the patch files.
Status Description	Describes the status of installation or uninstallation of the patch files.

This section contains the following:

Install Patch

To install the patch on your devices from Cisco DCNM Web Client, perform the following steps:

Procedure

-
- Step 1** Choose **Configure > Image Management > Patch [SMU] > Installation History**, click **Install**.
The **Select Switches** window appears. All the Cisco Nexus switches that are discovered by Cisco DCNM are displayed.
- Step 2** Select the check box to the left of a switch name.
You can select more than one device.
- Step 3** Click **Add** or **Remove** icons to include the appropriate switches for installing the patch.
The selected switches appear in the right column.

Step 4 Click **Next**.

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

The **SMU Package Browser** dialog box appears.

Step 6 In the **SMU Package Browser** dialog box, you can choose the patch file from **File Server** or **Switch File System**.

If you choose **File Server**:

- a) From the **Select the file server** list, choose the appropriate file server on which the patch is stored.

The servers, which are listed in the **Repositories** window, are displayed in the drop-down list. Choose **Configure > Image Management > Repositories** to view the **Repositories** window.

- b) From the **Select Image** list, choose the appropriate patch that must be installed on the device.

You can select more than one patch file to be installed on the device.

Note If the patch installation results in the restart of the device, select only one patch file.

Check the check box to use the same patch for all other selected devices of the same platform.

Only files with BIN extension are listed if you select **File Server**. To view other files, choose **Administration > DCNM Server > Server Properties**, set **FILE_SELECTION_FILTER** to **false**, and restart the server. It is set to **true** by default.

- c) From the **Select Vrf** list, choose the appropriate virtual routing and forwarding (VRF).

The two options in the drop-down list are **management** and **default**.

Check the check box to use the same VRF for all other selected devices.

- d) Click **OK** to choose the patch image or **Cancel** to revert to the SMU installation wizard.

If you choose **Switch File System**:

- a) From the **Select Image** list, choose the appropriate patch file image that is located on the flash memory of the device.

You can select more than one patch file to be installed on the device.

Only files with BIN extension are listed if you select **Switch File System**. To view other files, choose **Administration > DCNM Server > Server Properties**, set **FILE_SELECTION_FILTER** to **false**, and restart the server. It is set to **true** by default.

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

Step 7 Click **Finish**.

You will get a confirmation window. Click **OK**.

Note SMU installation may reload the switch if the SMU is reloaded.

You can view the list of patches that are installed on the switch in the **Switches** window by choosing **DCNM > Inventory > Switches**.

Uninstall Patch

To uninstall the patch on your devices from Cisco DCNM Web Client, perform the following steps:

Procedure

- Step 1** Choose **Configure > Image Management > Patch [SMU] > Installation History**, click **Uninstall**.
The **Select Switches** page appears. The discovered Cisco Nexus switches are displayed.
- Step 2** Check the check box on the left of the switch name.
You can select more than one image device.
- Step 3** Click **Add** or **Remove** icons to include the appropriate switches for installing the patch.
The selected switches appear in a column on the right.
- Step 4** Click **Next**.
The **Active Packages** page appears.
- Step 5** Click **Select Packages** under the **Installed Packages** column.
The **Packages Installed** window appears, which lists the patches that are applied to the switch.
- Step 6** Select the patches that you want to uninstall from this device.
You can select more than one patch that is applied on the device.
- Note** If the patch uninstallation results in the restart of the device, select only one patch.
- Step 7** Click **Finish** to uninstall the patch from the device.
You will get a confirmation window. Click **OK**.
You can uninstall more than one patch at a time.
- Note** SMU uninstallation may reload the switch if the SMU is reloaded.
-

Delete Patch Installation Tasks

To delete the patch installation tasks from the Cisco DCNM Web UI, perform the following steps:

Procedure

- Step 1** Choose **Configure > Image Management > Patch [SMU] > Installation History**, check the task ID check box.
- Step 2** Click **Delete**.
- Step 3** Click **OK** to confirm deletion of the patch installation task.
-

Switch Installed Patches

You can view the patches that are installed on all the switches in the network. You can refresh the view to see the latest installed patches.

The following table describes the fields that appear on **Configure > Image Management > Patch [SMU] > Switch Installed Patches**.

Field	Description
Switch Name	Specifies the name of the switch.
IP Address	Specifies the IP address of the switch.
Platform	Specifies the Cisco Nexus switch platform.
Installed Patches	Specifies the currently installed patches on switches.

Click **Refresh** to refresh the table.

Package [RPM]

The Package [RPM] menu includes the following submenus:

Package Installation [RPM]

The package [RPM] feature allows you to install RPM packages. This feature is available for the Cisco Nexus 9000 Series.

The following table describes the fields that appear on **Configure > Image Management > Package [RPM] > Installation History**.

Field	Description
Task Id	Specifies the serial number of the task. The latest task is listed in the top. The tasks are performed in the sequential order.
Switch Name	Specifies the name of the switch for which the package file is installed.
IPAddress	Specifies the IP address of the device.
Task	Specifies if the package is installed or uninstalled on this device.
Package	Specifies the name of the package file.
Status	Specifies the status of installation or uninstallation of the package files.
Completed Time	Specifies the time at which the installation or uninstallation task completed.

Field	Description
Status Description	Describes the status of installation or uninstallation of the package files.

This section contains the following:

Install Package [RPM]

Perform the following task to install the package on your devices using Cisco DCNM Web client.

Procedure

-
- Step 1** Choose **Configure > Image Management > Package [RPM] > Installation History**, click **Install**.
The **Select Switches** page appears.
- Step 2** Check the check box on the left of the switch name.
You can select more than one device.
- Step 3** Click **Add** or **Remove** to include appropriate switches for installing packaging.
The selected switches appear in a column on the right.
- Step 4** Click **Next**.
- Step 5** Click **Select Packages** in the **Packages** column.
The **RPM Package Browser** screen appears.
- Step 6** Choose the package file from **File Server** or **Switch File System**.
If you choose **File Server**:
- 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.
 - From the **Select Image** list, choose the appropriate package that must be installed on the device.
You can select more than one package file to be installed on the device.
Only files with RPM extension are listed if you select **File Server**. To view other files, choose **Administration > DCNM Server > Server Properties**, set **FILE_SELECTION_FILTER** to **false**, and restart the server. It is set to **true** by default.
Check the check box to use the same package for all other selected devices of the same platform.
 - Click **OK** to choose the patch image or **Cancel** to revert to the RPM Installation Wizard.
- If you choose **Switch File System**:
- From the **Select Image** list, choose the appropriate package file image that is located on the flash memory of the device.
You can select more than one package file to be installed on the device.

Only files with RPM extension are listed if you select **Switch File System**. To view other files, choose **Administration > DCNM Server > Server Properties**, set **FILE_SELECTION_FILTER** to **false**, and restart the server. It is set to **true** by default.

b) Click **OK**.

Step 7 In the **Installation Type** column, choose one of the installation types:

- **Normal**—Fresh installation
- **Upgrade**—Upgrading the existing RPM
- **Downgrade**—Downgrading the existing RPM

Step 8 Click **Finish**.

You can view the list of packages that are installed on the switch, on the **Web Client > Inventory > Switches** page.

Note If you are using Cisco DCNM Release 10.1(2), in case of installation of reload RPMs, perform a manual install commit on the switch after it switch reloads.

Uninstall Package [RPM]

To uninstall the RPM on your devices from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Configure > Image Management > Package [RPM] > Installation History**, click **Uninstall**. The **Select Switches** window appears.

Step 2 Check the check box on the left of the switch name.

You can select more than one switch.

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

The selected switches appear in a column on the right.

Step 4 Click **Next**.

The **Active Packages** page appears.

Step 5 Click **Select Packages** under the **Installed Packages** column.

The **Packages Installed** window appears, which lists the packages that are installed in the switch.

Step 6 Click **Finish** to uninstall the package from the device.

You will get a confirmation window. Click **OK**.

You can uninstall more than one package at a time.

Note

- If you are using Cisco DCNM Release 10.1(2), in case of uninstallation of reload RPMs, a manual install commit needs to be performed on the switch once the switch is reloaded.
- RPM uninstallation may reload the switch if the RPM is reload RPM.

Delete Package Installation Tasks

To delete the package installation tasks from the history view from the Cisco DCNM Web UI, perform the following steps:

Procedure

- Step 1** Choose **Configure > Image Management > Package [RPM] > Installation History**, select the task ID check box.
- Step 2** Click **Delete**.
- Step 3** Click **OK** to confirm deletion of the task.

Switch Installed Packages

You can view the RPM packages that are installed on all Switches in the network. You can refresh the view to see the latest installed packages.

The following table describes the fields that appear on **Configure > Image Management > Packages [RPM] > Switch Installed Packages**.

Field	Description
Switch Name	Specifies the name of the switch.
IP Address	Specifies the IP address of the switch.
Platform	Specifies the Cisco Nexus switch platform.
Installed Packages	Specifies the currently installed packages on the switches and the type of package. The installed packages can be base packages or non-base packages.

Click **Refresh** to refresh the table.

Maintenance Mode [GIR]

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

Maintenance Mode

The maintenance mode allows you to isolate the Cisco Nexus Switch from the network to perform an upgrade or debug, using Graceful Insertion and Removal (GIR). When the switch maintenance is complete, you can

return the switch to normal mode. When the switch is in the maintenance mode, all protocols are gracefully brought down and all physical ports are shut down. When the normal mode is restored, all the protocols and ports are initiated again.

Perform the following to change the system mode of the devices.

Procedure

Step 1 Choose **Configure > Image Management > Maintenance Mode [GIR] > Maintenance Mode**, check the switch name check box.

You can select multiple switches.

Step 2 Choose one of the following options under the **Mode Selection** column:

- Shutdown
- Isolate

Note Click the appropriate option before you change the mode.

Step 3 Click **Change System Mode**.

A confirmation message appears.

Step 4 Click **OK** to confirm to change the maintenance mode of the device.

The status of operation can be viewed in the **System Mode** and the **Maintenance Status**.

Switch Maintenance History

You can view the history of the maintenance mode changes executed from the Cisco DCNM.

The following table describes the fields that appear on **Configure > Image Management > Maintenance Mode [GIR] > Switch Maintenance History**.

Field	Description
Task Id	Specifies the serial number of the task. The latest tasks that are listed in the top.
Switch Name	Specifies the name of the switch for which the maintenance mode was changed.
IP Address	Specifies the IP address of the switch.
User	Specifies the name of the user who initiated the maintenance.
System Mode	Specifies the mode of the system.
Maintenance Status	Specifies the mode of the maintenance process.

Field	Description
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. <ul style="list-style-type: none"> • Planned • In Progress • Completed
KickStart Image	Specifies the kickstart image that is used to upgrade the Switch.
System Image	Specifies the system image that is used to upgrade the switch.
Completed Time	Specifies the date and time at which the upgrade was successfully completed.

Image and Configuration Servers

This feature allows you to upload or delete images that are used during POAP and switch upgrade. To view the **Image and Configuration Servers** window from the Cisco DCNM Web UI homepage, choose **Configure > Image Management > Repositories**.

You can view the following details in the **Image and Configuration Servers** window.

Field	Descriptions
Name	Specifies the name of the repository you upload.
URL	Specifies the path where you uploaded the repository.
Username	Specifies the username of the remote server.
Last Modified	Specifies the date and timestamp of the last modification.

Add Image or Configuration Server URL

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

Procedure

- Step 1** On the **Image and Configuration Servers** window, click the **Add** icon.
The **Add Image or Configuration Server URL** window is displayed.
- Step 2** Specify a name for the image.
- Step 3** Click the radio button to select the protocol.
The available protocols are **SCP**, **FTP**, **SFTP**, and **TFTP**. Use the SCP protocol for POAP and Image Management.
You can use IPv4 and IPv6 addresses with these protocols.
- Step 4** Enter the hostname or IP address and the path to download or upload files.
Note If you choose **SCP** or **SFTP** protocol and the path is root or /directory, adding an image or configuration server will not be successful.
- Step 5** Specify the username and password.
- Step 6** Click **OK** to save.
-

Deleting an Image

To delete an image from the repository from the Cisco DCNM Web UI, perform the following steps:

Procedure

- Step 1** Choose **Configure > Image Management > Repositories**.
The **Image and Configuration Servers** window appears.
- Step 2** Choose an existing image from the list and click the **Delete Image** icon.
A confirmation window appears.
- Step 3** Click **Yes** to delete the image.
-

Editing an Image or Configuration Server URL

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

Procedure

-
- Step 1** On the **Image and Configuration Servers** window, select an existing image and configuration server from the list, and click **Edit**.
- Step 2** In the **Edit Image or Configuration Server URL** window, edit the required fields.
- Step 3** Click **OK** to save or click **Cancel** to discard the changes.
-

File Browser

You can view the contents of the server on the **Image and Configuration Servers** page.

1. In the **Image and Configurations** page, check the **Server Name** check box to view the content.
2. Click **File Browser** to view the contents of this server.

Image Upload

To upload different types of images to the server from the Cisco DCNM Web UI, perform the following steps:



-
- Note** Devices use these images during POAP or image upgrade.
- Your user role should be **network-admin** to upload an image. You can't perform this operation with the **network-stager** user role.
-

Procedure

-
- Step 1** Choose **Configure > Image Management > Repositories**.
- The **Image and Configuration Servers** window appears.
- Step 2** Click **Image Upload**.
- The **Select File to Upload** dialog box appears.
- Step 3** Click **Choose file** to choose a file from the local repository of your device.
- Step 4** Choose the file and click **Upload**.
- Step 5** Click **OK**.
- The upload takes some time depending on the file size and network bandwidth.
-

LAN Telemetry Health

Starting from DCNM 11.2(1), Streaming LAN Telemetry preview feature in DCNM is obsolete and is replaced by Network Insights Resources (NIR) application. NIR can be deployed using Cisco DCNM Applications

Framework on **Web UI > Applications**. After the NIR is enabled on a fabric, you can monitor the status on the window in the Cisco DCNM Web UI.

When the connection status is shown as **Disconnected** the port configuration may not be accepted by the switch correctly. On the switch image 7.0(3)I7(6), if a switch already had **nxapi** configuration, and later it was managed by DCNM and telemetry was enabled on that fabric, DCNM pushes **http port 80** configuration so that it could query some NXAPI commands such as **show telemetry transport** and **show telemetry data collector details**, to monitor telemetry connection statistics. In this case, the switch does not update **http port 80** in its configuration even though the command was executed correctly. In such a scenario, issue the following commands on the switch:

```
switch# configure
switch(config)# no feature nxapi
switch(config)# feature nxapi
switch(config)# http port 80
```

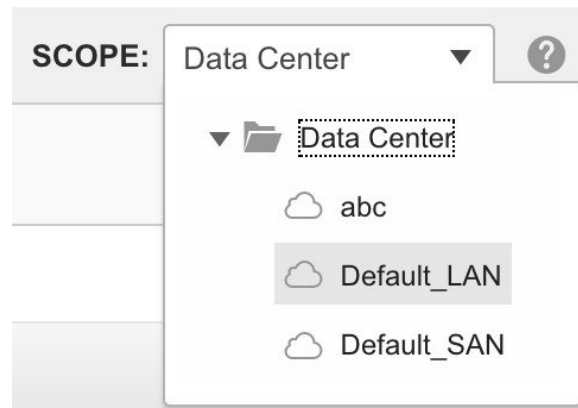


Note ICAM telemetry commands such as forwarding TCAM and ACL TCAM are not supported on Cisco Nexus C9504, C9508, and C9516 Series platforms for switch images 7.0(3)I7(5) and 7.0(3)I7(6)

LAN Telemetry has the following topics:

Health

Cisco DCNM allows you to monitor the configuration health attributes of Software Telemetry and Flow Telemetry for each fabric. The attributes are displayed for a particular fabric or all fabrics based on the selected **SCOPE**. **Data Center scope** displays all fabrics by default.



Software Telemetry

Data Center Network Manager										SCOPE: Data Center	admin
Control / LAN Telemetry / Health											
Software Telemetry Configuration Health 10 Total											
Fabric Name	Switch Name	Switch IP	Receiver IP Port	Receiver Status	Expected Config	Configuration Status	Sensor Status	Status Reason	Sensor Details		
DEF	gmurthy-spine3	15.15.15.25		—		—	—	Unsupported switch		
EXT	gmurthy-n9k-leaf3	15.15.15.10		—		—	—	Unsupported switch		
EXT	gmurthy-n9k-leaf2	15.15.15.9		—		FAILED	24	Sensor configuration...	...		
EXT	gmurthy-n9k-leaf1	15.15.15.8		—		FAILED	24	Sensor configuration...	...		
EXT-MON	gmurthy-n9k-leaf5	15.15.15.21	17.17.17.162:33002	—		MONITOR	—	Configure switch by f...	...		
EXT-MON	gmurthy-n9k-leaf4	15.15.15.20	17.17.17.162:33002	—		MONITOR	—	Configure switch by f...	...		
EXT-MON	7050SX-1	10.60.0.235		—		MONITOR	—	Third party switch ve...	...		
DEF	gmurthy-n9k-leaf7	15.15.15.26	17.17.17.162:33002	DISCONNECTED		SUCCESS	43	Receiver status reas...	...		
EXT	gmurthy-n9k-spine1	15.15.15.11	17.17.17.162:33002	—		SUCCESS	96	Fabric status will be *	...		
DEF	gmurthy-n9k-leaf6	15.15.15.23	17.17.17.162:33002	DISCONNECTED		SUCCESS	43	Receiver status reas...	...		

The following table describes the fields that appear in the **LAN Telemetry > Health > Software Telemetry** window.


Field	Description
Fabric Name	Displays the fabric name.
Switch Name	Displays the switch name.
Switch IP	Displays the switch management IP address.
Switch Serial	Displays the switch serial number. This column is hidden by default. Click the Settings icon, and check the Switch Serial check box to add it to the columns displayed.
Switch Model	Displays the switch model. This column is hidden by default. Click the Settings icon, and check the Switch Model check box to add it to the columns displayed.
Switch Version	Displays the switch image version. This column is hidden by default. Click the Settings icon, and check the Switch Version check box to add it to the columns displayed.
Receiver IP Port	Displays the receiver IP and port assigned to a switch to transport telemetry data. The assigned IP and port will be based on the configured telemetry network, out-of-band or in-band, and the corresponding receiver microservice that is running in NIR application.

Field	Description
Receiver Status	<p>Displays the status of the connection used to transport telemetry data between the switch and the receiver running in the NIR application.</p> <p>The telemetry manager polls the switch for the connection status every 5 mins.</p> <p>The valid values are:</p> <ul style="list-style-type: none"> • Connected: The status is Connected when the telemetry manager is able to poll the receiver connection status from the switches. • Disconnected: If the status is Disconnected, the reason is mentioned in the Status Reason column. • Null: The status is Null when the telemetry manager in DCNM has not polled the receiver connection status from the switches or when it has not received any response from the switch for that request. When the receiver status is Null and if the configuration status is MONITOR or SUCCESS, log into the switch and check the nxapi configuration. <p>When you enable telemetry on a fabric that is managed by DCNM, the telemetry manager pushes the httpport 80 configuration. If the switch does not have httpport 80 configuration, run the following commands on the switch:</p> <pre>switch# configure terminal switch(config)# no feature nxapi switch(config)# feature nxapi switch(config)# http port80</pre>
Configuration Type	<p>Displays the connection type ex: gRPC as reported by the switch. This value is obtained as part of the receiver connection status response from the switch. This column is hidden by default. It can be selected by clicking on the settings button.</p>

Field	Description
Expected Config	<p>Click the Expected Config icon to view the expected configuration for the switch in a dialog box. In case of error, the error reason will be displayed in the output.</p> <p>Expected Switch Configuration (Fabric: EXT, Switch: gmurthy-n9k-spine1)</p> <pre>configure terminal feature nxapi nxapi http port 80 feature ntp ntp server 15.15.15.162 prefer use-vrf management feature lldp feature icam feature telemetry telemetry destination-profile use-vrf default source-interface loopback0 destination-group 500 ip address 17.17.17.162 port 33002 protocol gRPC encoding GPB sensor-group 508 data-source DME path sys/intf depth 1 query-condition query-target=subtree&target-subtree-class= query-target-filter=deleted()</pre>

Field	Description
Configuration Status	<p>Displays the telemetry configuration switch summary status.</p> <p>The valid values are:</p> <ul style="list-style-type: none"> • MONITOR: Implies that the switch in the fabric was configured as Monitored in the NIR app. In this case, configure these switches manually with the telemetry configurations as displayed in the Expected Config column. • PROCESSING: Implies that the switch belonging to the fabric was configured as Managed in the NIR app. In this case, the telemetry manager will configure the switches and when configuration is in progress, it is displayed as PROCESSING. • SUCCESS: Implies that the switches were successfully configured. • PARTIAL SUCCESS: Implies that some of the telemetry configurations could not be pushed to the switches. The Status Reason column will indicate the failure reason. • FAILED: Implies that the DCNM job failed to configure the switches. It could happen that some configuration did get pushed to the switches while some did not, in that case also DCNM marks the whole job as Failed. The Status Reason column will indicate the failure reason. <p>You can filter the switches based on a particular status using the search option or you can sort the switches based on the status.</p> <p>Configuration Status ▾</p> <div> <div>SUCCESS</div> <div>SUCCESS</div> <div>SUCCESS</div> <div>MONITOR</div> <div>MONITOR</div> <div>MONITOR</div> </div>

Field	Description
Sensor Status	<p>Displays the sensor configuration status in a distributed color format. The sensor count is divided into three categories:</p> <ul style="list-style-type: none">• Green color (Success): Number of sensor paths that got configured successfully• Yellow color (Pending): Number of sensor paths that are pending to be configured• Red color (Failed): Number of sensor paths that could not be configured
Status Reason	<p>Displays the failure reasons for telemetry configuration status and receiver connection status or other information.</p>

Field	Description																									
Sensor Details	<div>Displays the following sensor details:</div> <ul style="list-style-type: none">• Group ID: The group ID to which the sensor path belongs• Name: The sensor path name as seen on the switch, for example: show processes cpu• Cadence (Seconds): The sample interval, in seconds, at which the switch streams that sensor path. For example: If the value is 60, every 60 seconds the switch shall stream that sensor metric.• Packets: Specifies the number of metric samples that is collected till time.• Job ID: This is the DCNM telemetry job ID that was used to configure the sensor path on the switch.• Status: The status of the job.• Status Reason: The status reason of the job. In case the job failed, it specifies the failure reason of that job. <div>Switch: gmurthy-n9k-leaf6, Fabric: DEF</div> <div>Sensor Details  43 Total</div> <table><thead><tr><th>Group ID</th><th>Name</th><th>Cadence (Seconds)</th><th>Packets</th><th>Job ID</th></tr></thead><tbody><tr><td>510</td><td>show interface hardwar...</td><td>32</td><td>11</td><td>59</td></tr><tr><td>510</td><td>show hosts</td><td>32</td><td>11</td><td>59</td></tr><tr><td>510</td><td>show lldp neighbors</td><td>32</td><td>11</td><td>59</td></tr><tr><td>510</td><td>show system internal elt...</td><td>32</td><td>11</td><td>59</td></tr></tbody></table>	Group ID	Name	Cadence (Seconds)	Packets	Job ID	510	show interface hardwar...	32	11	59	510	show hosts	32	11	59	510	show lldp neighbors	32	11	59	510	show system internal elt...	32	11	59
Group ID	Name	Cadence (Seconds)	Packets	Job ID																						
510	show interface hardwar...	32	11	59																						
510	show hosts	32	11	59																						
510	show lldp neighbors	32	11	59																						
510	show system internal elt...	32	11	59																						

Flow Telemetry

The screenshot shows the Cisco Data Center Network Manager interface. The breadcrumb navigation is 'Control / LAN Telemetry / Health'. Below this, there are tabs for 'Software Telemetry' and 'Flow Telemetry'. The main heading is 'Flow Telemetry Configuration Health' with a refresh icon and '4 Total' items. On the right, there are buttons for 'Retry All', a download icon, and a settings icon. The table below lists the configuration health for four switches.

Fabric Name	Switch Name	Switch IP	Exporter ID	Receiver IP Port	Expected Config	Overall Status	FT Setup Status	Flow Rules Status	Status Reason	Flow Rules
EXT-MON	gmurthy-n9k-leaf4	15.15.15.20	9	17.17.17.162:33000,17...		MONITOR	MONITOR	4 --		...
EXT-MON	gmurthy-n9k-leaf5	15.15.15.21	8	17.17.17.162:33000,17...		MONITOR	MONITOR	4 --		...
DEF	gmurthy-n9k-leaf6	15.15.15.23	10	17.17.17.162:33000,17...		SUCCESS	SUCCESS	4 --		...
DEF	gmurthy-n9k-leaf7	15.15.15.26	11	17.17.17.162:33000,17...		SUCCESS	SUCCESS	4 --		...

The following icons appear in the **LAN Telemetry > Health > Flow Telemetry** window.

- **Retry All:** Click the **Retry All** icon to retry the failed configurations on the switches. However, this option does not fix the issue for the unsupported configurations automatically.
- **Export:** Click the **Export** icon to download the data in a spreadsheet.
- **Settings:** Click the **Settings** icon to add or delete the columns you want to view.

The following table describes the columns in the **LAN Telemetry > Health > Flow Telemetry** tab.



Table 11: Fields and Description on Flow Telemetry Health tab








Field	Description
Fabric Name	Displays the name of the fabric.
Switch Name	Displays the name of the switch.
Switch IP	Displays the switch management IP address.
Switch Serial	Displays the serial number of the switch. By default, this column is hidden. It can be selected by clicking the Settings button.
Switch Model	Displays the switch model. By default, this column is hidden. It can be selected by clicking the Settings button.
Switch Version	Displays the switch image version. By default, this column is hidden. It can be selected by clicking the Settings button.
Exporter ID	Displays the exporter ID that is configured on the switch as part of the flow analytics configuration.

Field	Description
Receiver IP Port	Displays the comma-separated list of receiver IP addresses and ports assigned to a switch to transport flow telemetry data. The assigned IP addresses and ports will be that of the corresponding receiver microservices that are running in the NIR application and listening on the in-band network.
Expected Config	<p>On clicking, it displays the expected configuration for the switch in a pop-up window. In case of an error, the reason for the error is displayed in the output.</p> <p>Expected Switch Configuration (Fabric: DEF, Switch: gmur)</p> <pre> configure terminal ip access-list telemetryipv4acl 30 permit tcp 12.12.12.0/24 14.14.14.0/24 31 permit tcp 14.14.14.0/24 12.12.12.0/24 65535 deny ip any any exit ipv6 access-list telemetryipv6acl 32 permit udp 2001::/55 2003::/66 33 permit udp 2003::/66 2001::/55 65535 deny ipv6 any any exit feature analytics flow exporter telemetryExp_0 destination 17.17.17.162 use-vrf default transport udp 33000 source loopback0 dscp 44 flow exporter telemetryExp_1 destination 17.17.17.162 use-vrf default transport udp 33000 source loopback0 dscp 44 </pre>

Field	Description
Overall Status	

Field	Description
	<p>The flow telemetry configuration involves 2 components namely the Flow telemetry setup and Flow ACL configurations. The overall status column displays the summary of both these statuses. The following statuses are displayed:</p> <p>MONITOR: Implies that the switch in the fabric was configured as "Monitored" in the NIR app. In this case, it is your responsibility to configure these switches manually with the telemetry configurations as displayed in the Expected Config column.</p> <p>PROCESSING: This indicates that the switch belonging to the fabric was configured as "Managed" in the NIR app. In this case, the telemetry manager will configure the switches and when configuration is in progress, it is displayed as "PROCESSING".</p> <p>SUCCESS: This indicates that the switches were successfully configured.</p> <p>PARTIAL SUCCESS: This indicates that some of the telemetry configurations could not be pushed to the switches. The Status Reason column will indicate the failure reason.</p> <p>FAILED: This indicates that the DCNM job failed to configure the switches. It could happen that some configuration did get pushed to the switches while some did not, in that case also DCNM marks the whole job as Failed. The Status Reason column will indicate the failure reason.</p> <p>You can filter the switches based on a particular status using the search option (or) you can sort the switches based on the status.</p>

Field	Description
	<p>Overall Status  </p> <div> <div>MONITOR</div> <div>MONITOR</div> <div>SUCCESS</div> <div>SUCCESS</div> </div>
FT Setup Status	Displays the Flow telemetry setup status. If this shows Failed , it indicated that the flow analytics could not be enabled on the switches correctly and hence, the flow data cannot be exported from the switches.
Flow Rules Status (or) Flow ACL Status	<p>Displays the Flow ACL configuration status in a color-coded format.</p> <p>The flow rules status count is divided into 3 categories:</p> <ul style="list-style-type: none"> • Green (Success): Number of flow rules (ACEs) that got configured successfully. • Yellow (Pending): Number of flow rules (ACEs) that are pending to be configured. • Red (Failed): Number of flow rules (ACEs) that could not be configured.
Status Reason	Displays the failure reasons for the flow telemetry configuration (or) other information.

Field	Description															
Flow Rules	<div>Displays the following flow rule details:</div> <ul style="list-style-type: none">• ACL Name: The name of the access-list as configured on the switch. Only 2 ACLs get created namely telemetryipv4acl for IPv4 and telemetryipv6acl for IPv6.• Flow Rule#: This is the ACE rule number as configured within a particular ACL.• Flow Rule: This is the ACE rule that indicates the flow details like the protocol, source IP, source port, destination IP, destination port that should be exported.• Job ID: This is the DCNM telemetry job id that was used to configure the flow rules on the switch.• Status: The status of the job.• Reason: The status reason of the job. In case the job failed, it displays the failure reason of that job. If successful, it may show compliance and deployment successful in the case of Lan Fabric deployments. <div>Switch: gmurthy-n9k-leaf7, Fa</div> <div>Flow Rules  4 Total</div> <table><thead><tr><th>ACL Name </th><th>Flow Rule# </th><th>Flow Rule</th></tr></thead><tbody><tr><td>telemetryipv4acl</td><td>30</td><td>permit tcp 12.1..</td></tr><tr><td>telemetryipv4acl</td><td>31</td><td>permit tcp 14.1..</td></tr><tr><td>telemetryipv6acl</td><td>32</td><td>permit udp 200..</td></tr><tr><td>telemetryipv6acl</td><td>33</td><td>permit udp 200..</td></tr></tbody></table>	ACL Name 	Flow Rule# 	Flow Rule	telemetryipv4acl	30	permit tcp 12.1..	telemetryipv4acl	31	permit tcp 14.1..	telemetryipv6acl	32	permit udp 200..	telemetryipv6acl	33	permit udp 200..
ACL Name 	Flow Rule# 	Flow Rule														
telemetryipv4acl	30	permit tcp 12.1..														
telemetryipv4acl	31	permit tcp 14.1..														
telemetryipv6acl	32	permit udp 200..														
telemetryipv6acl	33	permit udp 200..														

**Note**

In case of MONITOR mode, you can configure flow telemetry on the switches using the following API that is available at <https://<dcnm-ip>/api-docs:/telemetry/switches/{serialNumber}/flow-analytics-config->> where serialNumber is the switch serial number as a string.

The Health table data gets refreshed every 70 seconds automatically. It can be manually refreshed by clicking the Refresh icon.