



Media Controller

This section describes the DCNM Media Controller.



Note This feature is available only if you have enabled the Media Controller feature explicitly, after the Cisco DCNM OVA/ISO installation is complete. For more information, see the *Cisco DCNM Installation Guide*.

This feature is available only if you have enabled Media Controller during the installation process. To enable Media Controller, you have to choose the **IP-Fabric Media Controller** installation option during the OVA/ISO installation for DCNM. The **appmgr set-mode media-controller** command, used in earlier releases, is not available in DCNM 10.4(2).

To bring up the devices from the basic configuration using POAP, you must define the templates and publish the POAP definition through Cisco DCNM **Web Client > Configure > Deploy > POAP Definitions**.



Note Specific POAP templates for Leaf and Spine for the Media Controller deployment are packaged with the Cisco DCNM Software.

If you have configured the Cisco DCNM server in Media Controller mode and performed the procedure that is mentioned in the "POAP Launchpad" section, you will be able to see the Media Controller templates. Cisco DCNM Web Client allows you to choose the required templates, edit them as required, and publish the POAP definition.

For information about the Media Controller APIs, see the [Cisco DCNM Media Controller API reference](#) on Cisco DevNet.

You can use the DCNM media controller deployment for only monitoring purposes and not as a policy manager. For more information, see *DCNM Read-Only Mode for Media Controller*.

NX-OS Streaming Telemetry and DCNM

Using streaming telemetry, NBM process on the switch informs DCNM its state using which DCNM is able to show discovered hosts and flows across the IP fabric. The POAP and `pmn_telemetry_snmp` CLI template, which are packaged in DCNM, generate the necessary telemetry configuration on the switch. An example of the generated configuration is as shown in the following sample:

```
telemetry
  destination-profile
```

```

    use-vrf management
destination-group 200
    ip address <dcnm-ip> port 50051 protocol gRPC encoding GPB
destination-group 1500
sensor-group 200
    data-source DME
    path sys/nbm/show/appliedpolicies depth unbounded
    path sys/nbm/show/stats depth unbounded
sensor-group 201
    data-source DME
    path sys/nbm/show/flows depth 0 query-condition
    rsp-subtree-filter=eq(nbmNbmFlow.bucket,"1")&rsp-subtree=full
sensor-group 202
    data-source DME
    path sys/nbm/show/flows depth 0 query-condition
    rsp-subtree-filter=eq(nbmNbmFlow.bucket,"2")&rsp-subtree=full
sensor-group 203
    data-source DME
    path sys/nbm/show/flows depth 0 query-condition
    rsp-subtree-filter=eq(nbmNbmFlow.bucket,"3")&rsp-subtree=full
sensor-group 204
    data-source DME
    path sys/nbm/show/flows depth 0 query-condition
    rsp-subtree-filter=eq(nbmNbmFlow.bucket,"4")&rsp-subtree=full
sensor-group 205
    data-source DME
    path sys/nbm/show/endpoints depth unbounded
sensor-group 300
    data-source NX-API
    path "show ptp brief"
    path "show ptp parent"
sensor-group 301
    data-source NX-API
    path "show ptp corrections"
sensor-group 500
    data-source NX-API
    path "show flow rtp details" depth 0
    path "show flow rtp errors active" depth 0
    path "show flow rtp errors history" depth 0
subscription 201
    dst-grp 200
    snsr-grp 200 sample-interval 60000
    snsr-grp 201 sample-interval 30000
    snsr-grp 205 sample-interval 30000
subscription 202
    dst-grp 200
    snsr-grp 202 sample-interval 30000
subscription 203
    dst-grp 200
    snsr-grp 203 sample-interval 30000
subscription 204
    dst-grp 200
    snsr-grp 204 sample-interval 30000
subscription 300
    dst-grp 200
    snsr-grp 300 sample-interval 30000
    snsr-grp 301 sample-interval 30000
subscription 500
    dst-grp 200
    snsr-grp 500 sample-interval 30000

```

- [Topology, on page 3](#)
- [PMN Hosts, on page 3](#)
- [Flow Alias, on page 6](#)

- [Policies, on page 9](#)
- [Flow Status, on page 18](#)
- [Events, on page 22](#)

Topology

You can view the Media Controller topology on the **Web UI > Media Controller > Topology** page. This topology is specific to the operations performed by DCNM as a Media Controller.



Note

- If you remove a device from the Inventory, the Policy deployment status for that switch is removed. However, clear the policy configuration on the switch also.

Quick Search

Enter the search string to highlight relevant devices.

The following fields are available to search on: **switch or hostname, switch or host IP address, switch MAC, and switch serial number**.

Multicast Group

Right-click (or press Return Key) in the field. A list of multicast addresses are displayed. You can choose the multicast IP address for which you need to view the topology.

The devices under this multicast IP address, and links to spine and leaf are highlighted. The dotted moving lines depict the flow of traffic in the Media Controller topology.

You can search or filter based on flow alias name in the Topology. When you search for Multicast Group, you can search using the IP address or flow alias name.

PMN Hosts

Cisco DCNM allows you to create hosts for Media Controller. The active transmitting and receiving devices are termed as hosts. The hosts can be configured on **Cisco Web Client > Media Controller > Hosts**.



Note

The PMN Hosts table is auto-populated once the traffic begins.

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

Table 1: Operations on PMN Hosts

Field	Description
Add	Allows you to add a new host.

Field	Description
Edit	Allows you to view or edit the selected host parameters.
Delete	Allows you to remove the host from the fabric.
Import	Allows you to import host parameters from your local directory.
Export	Allows you to export host parameters information to your local directory. The exported file is in <code>.csv</code> format.

Table 2: PMN Hosts Table Field and Description

Field	Description
Hostname	Specifies the configured name for the host device.
IP Address	Specifies the IP address for the host. Attention You should not create a host using a WAN interface IP address since any host policy that is subsequently created using the WAN interface IP address may result in unexpected behavior.
MAC Address	Specifies the MAC address of the host switch.
Switch Name	Specifies the name of the switch.
Interface Name	Specifies the name of switch interface which the host is associated with.
Remote Host	Specifies if the host is local to the DCNM managed fabric or belongs to an external fabric. A remote host can be identified by the Remote label on the host icon in the Topology page.

This section contains the following:



Note Starting from DCNM 10.4(2), the multisite option is supported. With this option, flows can be provisioned across multiple sites. You need to enable multisite support and receiver bandwidth management by setting the `pmn.multi-site.enabled` and `pmn.host.port.policing.enabled` functions to true, using the **Administration > DCNM Server > Server Properties** option, and restarting DCNM. The sender side bandwidth management for multisite is enforced by the switch and is enabled by default. Multisite support is only available for Source Specific Multicast (SSM), and border leaf switches. DCNM detects the PMN border leaf switch role during discovery and depicts the PMN border leaf switch separately on the topology screen.

Add PMN Hosts

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

-
- Step 1** Choose **Media controller > Hosts**.
The **Hosts** window is displayed.
- Step 2** Click the **Add** host icon.
- Step 3** In the **Add Hosts** window, specify the parameters in the following fields.
- **Name**: Specify a unique name for the host device.
 - **IP Address**: Specify the IP Address of the host device.
 - (Optional) **MAC Address**: Specify the MAC address of the host device.
- Step 4** Click **Save** to configure the host.
-

Edit PMN Hosts

To edit or view the host parameters from the Cisco DCNM Web UI, perform the following steps:

-
- Step 1** Choose **Media controller > Hosts**.
The **Hosts** window is displayed.
- Step 2** Check the check box next to the host name, that you need to edit.
- Step 3** Click **Edit** host icon.
- Step 4** In the Edit Hosts window, edit the parameters in the **Name** and **MAC Address** fields.
- Step 5** Click **Save** to save the changes. Click **Cancel** to revert the host with same parameters.
-

Delete PMN Hosts

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

-
- Step 1** Choose **Media controller > Hosts**.
The **Hosts** window is displayed.
- Step 2** Check the check box next to the hostname, to delete.
You can select more than one host to delete.
- Step 3** Click the **Delete** host icon.
- Step 4** In the delete notification, click **Yes** to delete the host. Click **No** to cancel this action.

A Delete Host successful message appears at the bottom of the page.

Import PMN Hosts

To import hosts, perform the steps below.

- Step 1** From the menu bar, select **Media Controller > Hosts**.
- Step 2** Click **Import** host icon.
- Step 3** Browse the directory and select the file which contains the Host configuration information.
- Step 4** Click **Open**.

The host(s) configuration is imported and displayed on **Media Controller > Hosts** on the Cisco DCNM Web Client.

Export PMN Hosts

To export hosts, perform the steps below.

- Step 1** From the menu bar, select **Media Controller > Hosts**.
- Step 2** Click **Export** host icon.
A notification window appears.
- Step 3** Select a location on your directory to store the Hosts configuration file.
- Step 4** Click **OK**.

The host(s) configuration file is exported to your local directory. The file name is appended with the date on which the file is exported. The format of the exported file is `.csv`.

Flow Alias

Using the Flow Alias feature, you can specify names for multicast groups. The multicast IP addresses are difficult to remember, thus by assigning a name to the multicast IP address, you can search and add policies based on the name.

You can configure a flow alias on **Media Controller > Flow Alias**.

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

Table 3: Flow Alias Table Field and Description

Field	Description
Flow Alias	Specifies the name of the Flow Alias.
Multicast IP Address	Specifies the multicast IP address for the traffic.
Description	Description added to the Flow Alias.
Last Updated at	Specifies the date on which the flow alias was last updated.

This section contains the following:

Add Flow Alias

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

-
- Step 1** Choose **Media controller > Flow Alias**.
The **Flow Alias** window is displayed.
- Step 2** Click the **Add** Flow Alias icon.
- Step 3** In the **Add Flow Alias** window, specify the parameters in the following fields.
- **Flow Name:** Specifies a unique flow alias name.
 - **Multicast IP Address:** Specifies the multicast IP Address for the flow alias.
 - **Description:** Specifies the description that you add for the flow alias.
- Step 4** Click **Save** to save the flow alias.
Click **Cancel** to discard.
-

Edit Flow Alias

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

-
- Step 1** Choose **Media controller > Flow Alias**.
The **Flow Alias** window is displayed.
- Step 2** Check the check box next to the flow alias name, that you need to edit.
- Step 3** Click **Edit** Flow Alias icon.
- Step 4** In the Edit Flow Alias window, edit the **Name**, **Multicast IP**, **Description** fields.
- Step 5** Click **Save** to save the new configuration.

Click **Cancel** to discard the changes.

Delete Flow Alias

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

- Step 1** Choose **Media controller > Flow Alias**.
The **Flow Alias** window is displayed.
- Step 2** Check the check box next to the flow alias, that you need to delete.
You can select more than one flow alias to delete.
- Step 3** Click **Delete Flow Alias** icon.
The flow alias is deleted.
-

Export Flow Alias

To export host alias from the Cisco DCNM Web UI, perform the following steps:

- Step 1** Choose **Media controller > Flow Alias**.
The **Flow Alias** window is displayed.
- Step 2** Click **Export** flow alias icon.
A notification window appears.
- Step 3** Select a location on your directory to store the Alias details file.
- Step 4** Click **OK**.
The flow alias file is exported to your local directory. The filename is appended with the date on which the file is exported. The format of the exported file is `.csv`.
-

Import Flow Alias

To import flow alias from the Cisco DCNM Web UI, perform the following steps:

- Step 1** Choose **Media controller > Flow Alias**.
The **Flow Alias** window is displayed.
- Step 2** Click **Import** flow alias icon.

Step 3 Browse the directory and select the file which contains the Flow Alias configuration information.

Step 4 Click **Open**.

The flow alias configuration is imported and displayed on the **Media controller > Flow Alias** window, on the Cisco DCNM Web Client.

Policies

Host Policies

You can add policies to the host devices. Navigate to **Media Controller > Policies > Host Policies** to configure the host policies.

By default, the sequence numbers for policies are auto-generated by DCNM and Multicast mask/prefix is taken as /32. The server property **pnm.hostpolicy.multicast-ranges.enabled** under **Administration > DCNM Server > Server Properties** must be set to 'true' for the user to be able to provide sequence numbers and multicast mask/prefix. When the server property is set to **True**, the fields to enter the sequence number and the multicast mask/prefix is available in the **Media Controller > Host > Host Policies > Add** and **Media Controller > Host > Host Policies > Edit** pages.

The default host policies must be deployed successfully to the switch before you deploy the custom host policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add, edit, import, or deploy custom policies.

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

Table 4: Host Policies Operations

Field	Description
Add	Allows you to add a new host policy.
Edit	Allows you to view or edit the selected host policy parameters.
Delete	<p>Allows you to delete the user-defined host policy.</p> <p>Note</p> <ul style="list-style-type: none"> • Undeploy policies from all switches before deleting them from DCNM. • You can undeploy the default policy, but you cannot delete the default policy. You can delete and undeploy only the custom policies. • When you undeploy the default policies, All Default Policies will be reset to have default permission (Allow).

Field	Description
Import	Allows you to import host policies from a CSV file to DCNM. Note After import, all policies imported from a CSV file are applied to all managed switches automatically.
Export	Allows you to export host policies from DCNM to a CSV file.

Table 5: Host Policies Table Field and Description

Field	Description
Policy Name	Specifies the policy name for the host, as defined by the user.
Host Name	Specifies the host ID.
Multicast IP	Specifies the multicast IP address for the host.
Flow Alias	Specifies the name of the Flow Alias.
Sender IP	Specifies the IP Address of the sender.
Host Acting As	Specifies the host device role. The host device role is either one of the following: <ul style="list-style-type: none"> • Sender • Receiver •
Operation	Specifies if the operation of the host policy. The policy has the following operations: <ul style="list-style-type: none"> • Permit • Deny
Sequence #	Specifies the sequence number of the custom policy when the multicast range is selected.
Deployment Action	Specifies the action performed on the switch for that host policy. <ul style="list-style-type: none"> • Create—The policy is deployed on the switch. • Delete—The policy is undeployed from the switch.
Devices Applied To	Specifies the number of devices to which this policy is applied.
PIM Policy	Specifies if Protocol Independent Multicast (PIM) configuration is applicable for the host policy.
Last Updated	Specifies the date and time at which the host policy was last updated. The format is <i>Day MMM DD YYYY HH:MM:SS Timezone</i> .

This section contains the following:

Add Host Policy

By default, the sequence number for policies is auto-generated by DCNM, and Multicast mask/prefix is /32 by default. The server property **pmn.hostpolicy.multicast-ranges.enabled** under **Administration > DCNM Server > Server Properties** must be set to 'true' for the user to be able to provide sequence numbers and multicast mask/prefix. When the server property is set to **true**, the fields to enter the sequence number and the multicast mask/prefix are available in the **Media Controller > Host > Host Policies > Add** and **Media Controller > Host > Host Policies > Edit** windows.

The default host policies must be deployed successfully to the switch before you deploy the custom host policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add custom policies.

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

Step 1 Choose **Media Controller > Policies > Host Policies**.

The **Host Policies** window is displayed.

Step 2 Click the **Add** icon.

Step 3 In the Add Host Policy window, specify the parameters in the following fields.

- **Policy Name:** Specifies a unique policy name for the host policy.
- **Host Role:** Specifies the host as a multicast sender or receiver. Select one of the following:
 - Sender
 - Receiver-Local
 - Receiver-External
- **PIM Policy:** Select the check box if PIM configuration is needed for the host policy. The PIM Policy checkbox is only applicable for the receiver role. If PIM policy is enabled, the Host field is disabled since the PIM policy is only applicable for the receiver and it is applied to the multicast group.
- **Host:** Specifies the host to which the policy is applied. If a destination host is detected, you can choose the hostname from the drop-down list.

Note Do not select hosts that are discovered as remote receivers to create receiver or sender host policies. However, hosts that are discovered as remote senders can be used for creating sender host policies.
- **Multicast IP:** Specifies the multicast IP Address for the host policy.
- **Allow/Deny:** Click the radio button to choose, if the policy must **Allow** or **Deny** the traffic flow.

Step 4 Click **Save** to configure the host policy.

Step 5 Click **Save & Deploy** to configure and deploy the Policy.

Click to discard the new policy.

Edit Host Policy

The default host policies must be deployed successfully to the switch before you deploy the custom host policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you edit custom policies.

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

Step 1 Choose **Media Controller > Policies > Host Policies**.

The **Host Policies** window is displayed.

Step 2 Check the check box next to the host policy name, that you need to edit.

Step 3 Click **Edit** Host policy icon.

Step 4 In the Edit Host Policy window, edit to specify if the policy will **Allow** or **Deny** traffic.

Note The changes made to Host Policy are applied immediately. If the policy is already applied to any device, the changes may impact the existing flows.

Step 5 Click **Save** to save the new configuration.

Step 6 Click **Save & Deploy** to configure and deploy the Policy.

Click to discard the changes.

Delete Host Policy

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



Note You can delete only user-defined Host Policies.

Step 1 Choose **Media Controller > Policies > Host Policies**.

The **Host Policies** window is displayed.

Step 2 Check the check box next to the host policy name, that you need to delete.

You can select more than one host policy to delete.

Step 3 Click **Delete** Host policy icon.

Step 4 In the delete notification, click **OK** to delete the host policy. Click **Cancel** to return to the Host Policies page.

Note Deleting a host policy from DCNM does not undeploy the policy from the switches on which it is deployed. It is highly recommended to undeploy the policy on the switches before deleting it from DCNM.

A Delete Host policy successful message appears at the bottom of the page.

Import Host Policy

The default host policies must be deployed successfully to the switch before you deploy the custom host policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add custom policies.

To import host policies from the Cisco DCNM Web UI, perform the following steps:

-
- Step 1** Choose **Media Controller > Policies > Host Policies**.
The **Host Policies** window is displayed.
- Step 2** Click the **Import** host policy icon.
- Step 3** Browse the directory and select the `.csv` format file which contains the Host Policy configuration information.
The policy will not be imported if the format in the `.csv` file is incorrect.
- Step 4** Click **Open**.
The imported policies are automatically deployed to all the switches in the fabric.
-

Export Host Policy

To export host policies from the Cisco DCNM Web UI, perform the following steps:

-
- Step 1** Choose **Media Controller > Policies > Host Policies**.
The **Host Policies** window is displayed.
- Step 2** Click the **Export** host policy icon.
A notification window appears.
- Step 3** Select a location on your directory to store the Host Policy details file.
- Step 4** Click **OK**.
The host policy file is exported to your local directory. The filename is appended with the date on which the file is exported. The format of the exported file is `.csv`.
-

Flow Policies

You can configure the flow policies on **Media controller > Flow Policies**.

The default policies are displayed on the Flow policy page. By default, the bandwidth of these policies is 0. You can configure the bandwidth such that any flow that matches the default flow policy will accordingly use the bandwidth and QOS/DSCP parameters. The policy is deployed to all the devices when you save the configuration.

The default flow policies must be deployed successfully to the switch before you deploy the custom flow policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add, edit, import, or deploy custom policies.



Note When you undeploy a default policy, it will be reset to default values, that is, Bandwidth:0gbps, DSCP:Best Effort, and Policer:Enabled.

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

Table 6: Flow Policies Operations

Field	Description
Add	Allows you to add a new flow policy.
Edit	Allows you to view or edit the selected flow policy parameters.
Delete	Allows you to delete the user-defined flow policy. Note <ul style="list-style-type: none"> • You cannot delete the default flow policies. • Undeploy policies from all switches before deleting them from DCNM.
Import	Allows you to import flow policies from a CSV file. Note After import, all policies imported from a CSV file are applied to all managed switches automatically.
Export	Allows you to export flow policies to a CSV file.

Table 7: Flow Policies Table Field and Description

Field	Description
Policy Name	Specifies the flow policy name.
Multicast IP	Specifies the multicast IP address for the traffic.
Flow Alias	Specifies the name of the Flow Alias.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.
QoS/DSCP	Specifies the Switch-defined QoS Policy.

Field	Description
Deployment Action	Specifies the action that is performed on the switch for that host policy. <ul style="list-style-type: none"> • Create—The policy is deployed on the switch. • Delete—The policy is undeployed from the switch.
Last Updated	Specifies the date and time at which the flow policy was last updated. The format is <i>Day MMM DD YYYY HH:MM:SS Timezone</i> .



- Note** A new flow policy or an edited flow policy is effective only under the following circumstances.
- If the new flow matches the existing flow policy.
 - If the flow expires and reforms, while the new policy is already added or edited, that matches with the flow policy.

This section contains the following:

Add Flow Policy

The default host policies must be deployed successfully to the switch before you deploy the custom host policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add custom policies.

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

-
- Step 1** Choose **Media controller > Flow Policies**.
The **Flow Policies** window is displayed.
- Step 2** Click the **Add Flow** policy icon.
- Step 3** In the Add Flow Policy window, specify the parameters in the following fields.
- **Policy Name**: Specifies a unique policy name for the flow policy.
 - **Multicast IP**: Specifies the multicast IP Address for the flow policy.
 - **Bandwidth**: Specifies the bandwidth that is allocated for the flow policy. Select of the radio buttons to choose **Gbps** or **Mbps**.
- Step 4** From the **QoS/DSCP** drop-down list, choose an appropriate ENUM value.
- Step 5** Click **Save** to configure the flow policy.
-

Edit Flow Policy

The default flow policies must be deployed successfully to the switch before you deploy the custom flow policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you edit custom policies.

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

SUMMARY STEPS

1. Choose **Media controller > Flow Policies**.
2. Check the check box next to the flow policy name, that you need to edit.
3. Click **Edit** Flow policy icon.
4. In the Edit Flow Policy window, edit the **Multicast IP**, **Bandwidth**, **QoS/DSCP** fields.
5. Click **Save** to configure the flow policy.

DETAILED STEPS

-
- Step 1** Choose **Media controller > Flow Policies**.
The **Flow Policies** window is displayed.
- Step 2** Check the check box next to the flow policy name, that you need to edit.
- Step 3** Click **Edit** Flow policy icon.
- Step 4** In the Edit Flow Policy window, edit the **Multicast IP**, **Bandwidth**, **QoS/DSCP** fields.
- Step 5** Click **Save** to configure the flow policy.
-

Delete Flow Policy

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

-
- Step 1** Choose **Media controller > Flow Policies**.
The **Flow Policies** window is displayed.
- Step 2** Check the check box next to the flow policy name, that you need to delete.
You can select more than one flow policy to delete.
Note You cannot delete the default policies.
- Step 3** Click **Delete** icon to delete the selected flow policy.
Click **Delete All** icon to delete all the flow policies at a single instance.
-

Import Flow Policy

The default flow policies must be deployed successfully to the switch before you deploy the custom flow policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you import custom policies.

To import flow policies from the Cisco DCNM Web UI, perform the following steps:

SUMMARY STEPS

1. Choose **Media controller > Flow Policies**.
2. Click the **Import** flow policy icon.
3. Browse the directory and select the file which contains the Flow Policy configuration information.
4. Click **Open**.

DETAILED STEPS

Step 1 Choose **Media controller > Flow Policies**.

The **Flow Policies** window is displayed.

Step 2 Click the **Import** flow policy icon.

Step 3 Browse the directory and select the file which contains the Flow Policy configuration information.

Step 4 Click **Open**.

The flow policy configuration is imported and displayed on the **Media controller > Flow Policies** window, on the Cisco DCNM Web Client.

The imported policies are automatically deployed to all the switches in the fabric.

Export Flow Policy

To export host policies from the Cisco DCNM Web UI, perform the following steps:

Step 1 Choose **Media controller > Flow Policies**.

The **Flow Policies** window is displayed.

Step 2 Click the **Export** flow policy icon.

A notification window appears.

Step 3 Select a location on your directory to store the Flow Policy details file.

Step 4 Click **OK**.

The flow policy file is exported to your local directory. The filename is appended with the date on which the file is exported. The format of the exported file is `.csv`.

Flow Status

Cisco DCNM allows you to view the flow status pictorially and statistically. The flow status is available on **Media Controller > Flow Status**.



Note The flow status collection frequency and cache size can be specified via **cisco.pmn-stats-interval** and **cisco.pmn-stats-cache-size** respectively in the **Administration > DCNM Server > Server Properties** page.

Fields and Descriptions

The following table describes the fields that appear on the Active tab.

Table 8: Active Tab

Field	Description
Show Chart	<p>Click Show Chart icon to view the graphical representation of the Flow Status.</p> <p>Note The data refers to the sender leaf when the sender starts broadcasting. See the receiver start time in the flow status table to find when the receiver started getting data.</p> <p>Click the Show drop-down list to view the flow status information in one of the following formats—Chart, Table, or Chart and Table.</p> <p>Click Chart Type icon to view the various chart types. Select a chart type to view the flow status information that is depicted in that chart format. You can choose a chart option to see filled patterns or data markers.</p> <p>Click Actions icon to print the report or excel chart information to your local directory.</p>
Multicast IP	<p>Specifies the multicast IP address for the flow.</p> <p>Note You can click the wave link next to the Multicast IP address to view the pictorial representation of flow statistics.</p>
Flow Alias	Specifies the name of the Flow Alias.
Sender	Specifies the IP Address or the Host alias of the sender for the multicast group.
Receiver	Specifies the IP Address or the Host alias of the receiver joining the group.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.

Field	Description
QOS/DSCP	Specifies the Switch-defined QoS Policy.
Flow Link State	Specifies the state of the flow link. Click READY link state to view the network diagram of the Sender and Receiver.
Policy ID	Specifies the policy ID applied to the multicast IP.
Receiver Start Time	Displays the time from when the receiver begins to receive data.

The following table describes the fields that appear on the Inactive tab.

Table 9: Inactive Tab

Field	Description
Show Chart	Click Show Chart icon to view the graphical representation of the Flow Status. Note The data refers to the sender leaf when the sender starts broadcasting. Please see the receiver start time in the flow status table to find when the receiver started getting data. Click the Show drop-down list to view the flow status information in one of the following formats—Chart, Table, or Chart and Table. Click Chart Type icon to view the various chart types. Select a chart type to view the flow status information that is depicted in that chart format. You can choose a chart option to see filled patterns or data markers. Click Actions icon to print the report or excel chart information to your local directory.
Multicast IP	Specifies the multicast IP address of the flow.
Flow Alias	Specifies the name of the Flow Alias.
Sender	Specifies the IP Address or the Host alias of the sender for the multicast groups.
Receiver	Specifies the IP Address or the Host alias of the receiver.
Waiting Receivers	Specifies the potential multicast receivers that have subscribed to this group.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.

Field	Description
Flow Link State	Click the READY link state to view the network diagram of the Sender and Receiver. The dotted line displays the direction of the flow of traffic.
Policy ID	Specifies the policy ID applied to the multicast IP.
Fault Reason	Specifies reason for the inactive flow. Cisco DCNM determines the inactive flow if both the sender and receiver mroute exists with any of the following combinations. <ul style="list-style-type: none"> • Receiver IIF is null • Receiver OIF is null • Sender IIF is null • Sender OIF is null <p>In this scenario, the switch won't have any fault reason. Therefore, there's no fault reason for such inactive flows.</p>

The following table describes the fields that appear on the Sender Only tab.

Table 10: Sender Only Tab

Field	Description
Multicast IP	Specifies the multicast IP address for the flow.
Flow Alias	Specifies the name of the Flow Alias.
Name	Specifies the name of the sender.
Sender Leaf IP	Specifies the IP address of the sender that initiates the multicast flow.
Sender Leaf Name	Specifies the name of the sender leaf.
Sender Switch	Specifies the IP address of the sender switch.
Sender Ingress Interface	Specifies the name of the sender ingress interface.
Flow Link State	Specifies the flow link state, if it is allow or deny.
Policy ID	Specifies the policy ID applied to the multicast IP.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.
State	Specifies the state of the flow link.

The following table describes the fields that appear on the Receiver Only tab.

Table 11: Receiver Only Tab

Field	Description
Multicast IP	Specifies the multicast IP address for the flow.
Flow Alias	Specifies the name of the Flow Alias.
Name	Specifies the receiver ID. If the multicast receiver is remote, the Remote label can be seen next to its name.
Receiver Leaf IP	Specifies the IP address of the destination switch that receives the multicast flow.
Receiver Interface	Specifies the name of the destination switch interface.
Receiver Switch	Specifies the IP address of the receiver switch.
Receiver Leaf Name	Specifies the name of the leaf switch to which the multicast receiver is attached.
Source Specific Sender	Specifies the IP address of the multicast sender.
Policy ID	Specifies the policy ID applied to the multicast IP.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.
Receiver Join Time	Specifies the time at which the receiver joined.
Number of Receivers	Specifies the number of receivers that are allotted for the traffic.
State	Specifies the state of the flow link.

Click the **Show** drop-down list in the statistical representation area to display the statistical data in various formats.

Click the arrow to export the statistical data. You can export it in `.csv` or `.pdf` formats.



Note Cisco DCNM holds the Flow statistics values in the DCNM server internal memory. Therefore, after a DCNM Restart or HA switch over, the Flow statistics won't show previously collected values. However, you can see the Flow statistics that are collected after the server Restart or HA switch over.

If the new flow joins before the uplinks between the switches that are detected in DCNM, a message `BW_UNAVAIL` appears. This is resolved after the uplinks between the switches are detected by DCNM after discovery of the devices.

Events

Cisco DCNM allows you to view and purge the various events between the Host and Flow. The Events are recorded on **Media Controller > Events**.

The PMN Events table is updated real-time.

The maximum stored PMN events and cleanup frequency can be specified via **pnn.rows.limit** and **pnn.delete.interval** respectively in the **Administration > DCNM Server > Server Properties** page.

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

Field	Description
Purge	<p>Click to remove the old/unwanted events.</p> <p>Note If the DCNM server restarts, by default a maximum of 5000 event entries are retained for 6 hours.</p> <p>Click one of the radio buttons to choose the Purge options.</p> <ul style="list-style-type: none"> • Max # of Records—Enter the maximum number of records to delete. • # of Days—Enter the number of days for which you need to delete the events. • Delete all data from the previous date—Specifies a date before which all the data is deleted. <p>Click Purge to delete/retain PMN events information.</p>
Category	Specifies if the event category.
Severity	Specifies the severity of the event.
Description	<p>Specifies the description of the event.</p> <p>The sample description appears as:</p> <pre>Creating flow for FlowRequest:The flowRequest is for hostId:<<IP_Address>> hostInterface:<<Host_Int_ID>> mcastIp:<<Multicast IP>> Is sender role:false originating from switch:<<Host IP Address>></pre>
Impacted Flows	Specifies the impacted flows due to this event.
Last Update Time	<p>Specifies the date and time at which the event was last modified.</p> <p>The format is <i>Day MMM DD YYYY HH:MM:SS Timezone</i>.</p>
Export	<p>Allows you to download the events to a local directory path.</p> <p>The filename is appended with the date on which the file is exported. The format of the exported file is <i>.xls</i>.</p>