USER GUIDE

Brocade Flow Optimizer User Guide

Supporting Brocade Flow Optimizer 1.2

9 May 2016

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit http://www.brocade.com/support/oscd.

Contents

About this Document

What's new in this document

The following table describes information added to this guide for Brocade Flow Optimizer release 1.2.0.

TABLE 1 Summary of enhancements in Brocade Flow Optimizer release 1.2.0

Feature	Description	Location
HTTPS communication between Brocade Flow Optimizer and SDN Controller	A new check box in the **SDN Controller Settings** dialog box allows you to set up HTTPS communication between the Brocade Flow Optimizer and the SDN Controller.	Setting up the connection to the SDN Controller on page 16
Flow naming	The **Add Custom Flow** dialog box has a new field, **Flow Name**, for both user-defined and learned flows. You can now search on the flow name in both the **Learned Flows** and **User Defined Flows** tabs.	Add Custom Flow dialog on page 62 Learned Flows tab on page 60 User Defined Flows tab on page 61
Support ingress port for Drop and Redirect action	You can now configure an ingress port in the **Node Ports Picker** dialog box if the action is Drop or Redirect.	Node Ports Picker dialog on page 67
SDN-based flow tap	When configuring a user-defined flow or a custom profile, you can select up to three mitigation actions, to create an end-to-end automated flow path for the traffic to reach third-party tools to further analyze the traffic. You can also override or remove the original match criteria.	Add Custom Flow dialog on page 62 Add Custom Profile dialog on page 65 Edit Profile dialog on page 69 Node Ports Picker dialog on page 67
Ether Type as a match criteria	When configuring a custom profile, you can select Ether Type as a match criteria.	Add Custom Profile dialog on page 65 Edit Profile dialog on page 69
VLAN Modify and VLAN Pop	In the **Node Ports Picker** dialog box, you can now select VLAN actions Modify and Pop. You can also specify a VLAN ID.	Node Ports Picker dialog on page 67
Support for L2 mask for the MAC address	When creating or editing a profile or a flow, the MAC address can include a mask.	Add Custom Flow dialog on page 62 Add Custom Profile dialog on page 65 Edit Profile dialog on page 69
Display IPSec header information for Learned flows	In the **Learned Flows** tab of the **Flows** page, you can select whether to display IPSec header information in the list of flows.	Learned Flows tab on page 60
Display OpenFlow statistics for User Defined flows and Learned & Programmed flows.	In the **User Defined Flows** tab and the **Learned & Programmed Flows** tab, you can display OpenFlow statistics (byte count, packet count) for the flows.	User Defined Flows tab on page 61 Learned and Programmed Flows tab on page 59
Bulk deletion of user-defined flows	In the **User Defined Flows** tab of the **Flows** page, in addition to being able to delete flows individually, you can now select and delete several flows at once.	Deleting user-defined flows on page 51

TABLE 1 Summary of enhancements in Brocade Flow Optimizer release 1.2.0 (continued)

Feature	Description	Location
Large flow inactive limit	In the configuration file, you can specify a time after which inactive large flows are automatically deleted from the database.	Changing the inactive time limit for large flows on page 51
System resource validation	The startservice script now validates your configuration with the minimum and recommended configuration.	Starting the Brocade Flow Optimizer application on page 11

Supported hardware and software

Make sure your system meets the requirements for installation and use of the Brocade Flow Optimizer application.

TABLE 2 System requirements

Item	Requirement
Host server	Linux operating system (one of the following): • Ubuntu 14.0.4 (64 bit) • CentOS 7 (64 bit) The server must have in-band connectivity to receive sFlow packets from MLX devices.
Memory and hard disk drive	• 16 GB RAM • 255 GB of free HDD space • A minimum of 4 core processors
Brocade devices	One or more of the following: • Brocade ICX 7250 • Brocade ICX 7450 • Brocade ICX 7750 • Brocade MLXe
Software	The firmware requirements vary depending on the device: • For ICX 7450 and ICX 7750: – FastIron 8.0.40a • For MLXe: – NetIron 5.9a (for generic support) – NetIron 6.0 (for MPLS LSP Logical Port) – NetIron 5.9b and 6.0 (for IPsec) • OpenFlow version 1.3
OpenFlow controller	One of the following: • Brocade SDN Controller, version 2.3.0 • OpenDaylight (ODL), Lithium SR3 You can download the Brocade SDN Controller from http://www.my.brocade.com.
Browser	Google Chrome

Getting Started

Introduction to Brocade Flow Optimizer

The Brocade Flow Optimizer application enables you to optimize the traffic flows on your network by providing the ability to monitor and control flows that exceed the bandwidth utilization you have established for the flows.

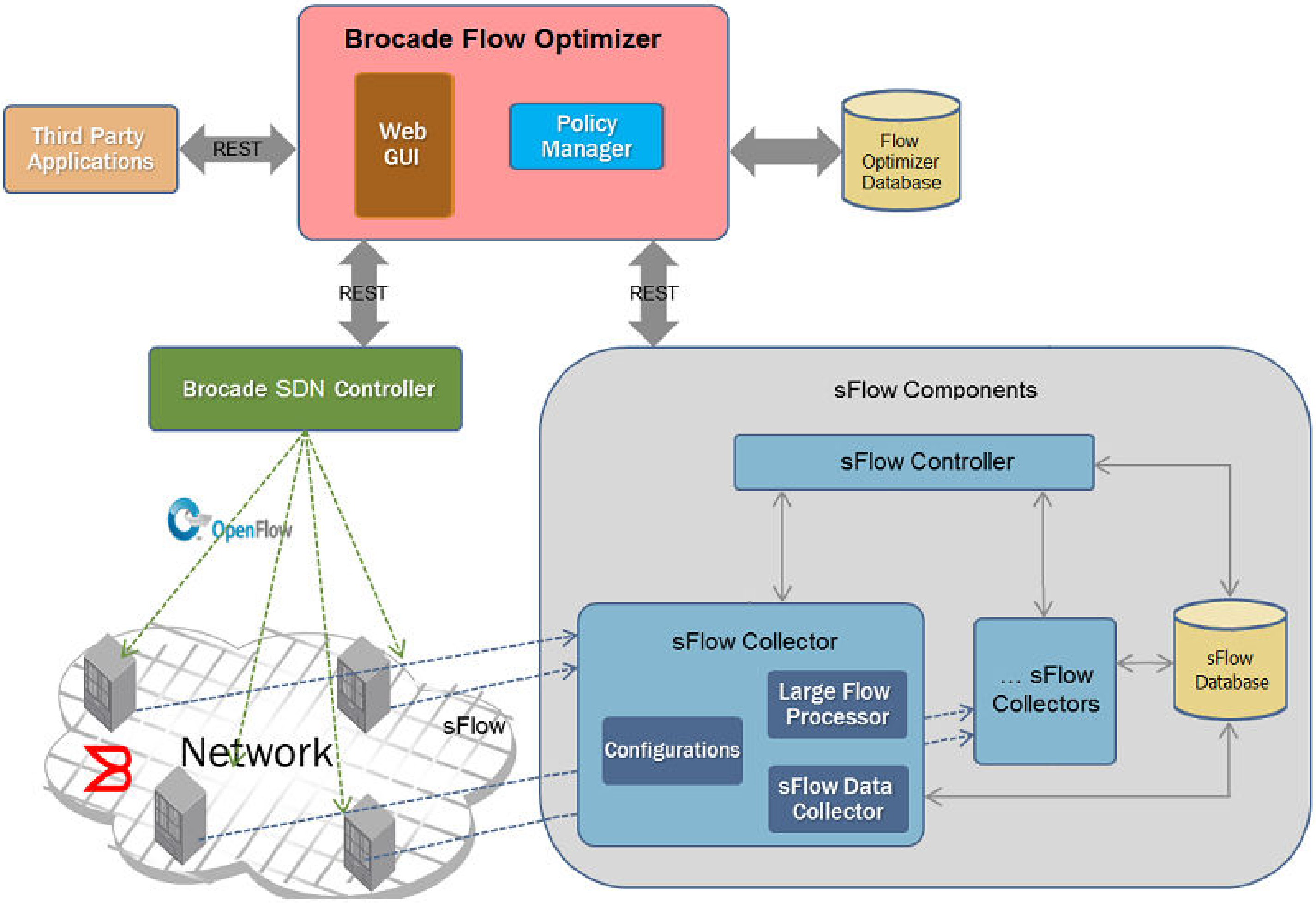
Monitoring traffic flows enables you to identify different types of volumetric traffic that exceed the bandwidth utilization thresholds you have established for the traffic. Once the out-of-range volumetric traffic has been identified, you can enforce your traffic management policy by choosing to drop, redirect, mirror, or meter the out-of-range volumetric traffic.

The Brocade Flow Optimizer application monitors sFlow traffic on OpenFlow-enabled ports using the Brocade SDN Controller (BSC), or the community Helium OpenDaylight (ODL) controller. The application provides configurable traffic monitoring templates (called profiles) that you use to monitor different types of traffic. It also provides configurable parameters that enable you to set thresholds for the different types of volumetric traffic and to specify the mitigation action for each traffic type.

The application provides a dashboard that enables you to easily view real-time volumetric traffic, real-time events, and the current set of profiles that are available for monitoring traffic. The dashboard also provides access to the options used to configure and edit traffic profiles.

The following figure shows the basic architecture of a typical system implementation of the Brocade Flow Optimizer application.

FIGURE 1 Brocade Flow Optimizer basic architecture



Limitations

This release of the Brocade Flow Optimizer has the following limitations.

All ICX devices

The known limitations for this release are as follows:

- **Operational API support during flow creation:** When creating flows on the device, operational API is either returning empty, or the flow name is invalid. This makes the operational API unusable. To prevent this, disable the operational API check. To do this, set the **compare.configured.and.operational.flows** property to 'false', before you run the **./startservice** script to start the application.

  The **compare.configured.and.operational.flows** property is in the *config.properties* file located at *<install_location> \flow_optimizer_1.1\configuration*.

ICX 7450 and ICX 7750

The known limitations for this release are as follows:

- **OpenFlows with layer 3 (L3) Source IP:** Flows that are defined with L3 Source IP are rejected by the device. The device returns this error message: *FLOW MOD ERROR: Status: ERROR: Reason: Error: L2Flow enabled Ports does not accept L3Flow.*
- **DSCP Remark for Meter flows:** Meter flows with DSCP remark are rejected by the device. The device returns this error message: *METER MOD ERROR: Status: ERROR: Reason: Meter id: <ID> Band not supported.*

Flows

The known limitations for this release are as follows:

- The same metered flow cannot be configured on multiple ingress ports. You can configure multiple, independent metered flows on a single ingress port.
- Metered flows are not removed when the bandwidth utilization falls below the Threshold value you specified for the flow. To remove the metered flow, you must disable or delete the profile.

Profiles

The known limitations for this release are as follows:

- **Editing, disabling, or deleting profiles:** These operations reset the flows associated with the deleted profile.

Starting the Brocade Flow Optimizer application

You must start the Brocade Flow Optimizer application on the host server before any clients can log in.

Pre-requisites: The application must be installed on the host server, and you must have access to the server.

Ensure that your system meets the requirements as listed in Supported hardware and software on page 8

When you run the **startservice** script to start the Brocade Flow Optimizer, it validates your system configuration with the minimum and recommended configuration.

- If the minimum configuration is not met, and error is displayed and the Brocade Flow Optimizer will not start.
- If the recommended configuration is not met, a warning is displayed, and you are given the option to continue with installation anyway.

You can optionally suppress this validation check using the -i parameter of the **startservice** script.

Complete these steps to start the application.

1. Go to the home directory (where the application files were installed).
2. Open the `/bin` folder.
3. Optional: Use one of the following commands to check the available and recommended system configuration.
   - (Root user): **sh startservice -c**, or **./startservice -c**
   - (Non-root user): **sudo sh startservice -c**, or **sudo ./startservice -c**

   The available and recommended configurations are displayed.
4. Use one of the following commands to run the **startservice** script (this starts the application):
   - (Root user): **sh startservice**, or **./startservice**
   - (Non-root user): **sudo sh startservice**, or **sudo ./startservice**

Log in to the application to verify that it is installed correctly. If this is a first-time installation, you must log in and then complete the initial system configuration tasks.

Logging in to the Brocade Flow Optimizer client

Before you can begin using the Brocade Flow Optimizer, you must log in using the web client. The login process is the same regardless of whether you have Administrator or Operator privileges.

> NOTE
> When the Brocade Flow Optimizer software is installed, an Administrator user is automatically created.

Complete the following steps to login.

1. Open your browser and point it to the following URL:

   https://<IP address of server>:8089/

   The port number must be 8089. This is the port number for the Brocade Flow Optimizer application.

   A page appears with an alert about a security certificate or that the connection may not be secure.
2. Select or click the option to continue with the connection.
   The **Login** page appears.
3. Type your username and password in the appropriate fields.

   If you are an Administrator and are logging in for the first time, use the default username and password.

   - **Username**: Administrator
   - **Password**: password

   You can change the password later.
4. Press **Enter** or click the **arrow button**.
   The **Dashboard** page of the Brocade Flow Optimizer application appears.

The application session starts with the **Dashboard** page displayed. If there is no user activity for 30 minutes after the session starts, the session times out (closes) and you must log in again.

Initial system configuration

Once you have completed the installation of the required software and the Brocade Flow Optimizer application software, you need to configure the system so that the system components are logically connected.

The system configuration process must be completed to ensure that system devices can exchange messages and data during normal operations and that the Brocade Flow Optimizer is able to receive sample flows to be monitored.

The system configuration involves the following basic tasks:

- One of the following, based on the Controller you are using:
  - **Brocade SDN Controller:** Enabling Host Tracker No Flood Hybrid Mode on the BSC Controller on page 13
  - **OpenDayLight:** Enabling Host Tracker No Flood Hybrid Mode on the ODL Controller on page 13
- Enabling OpenFlow on MLX routers on page 14
- Enabling OpenFlow on ICX devices on page 15
- Setting up the connection to the SDN Controller on page 16
- Configuring the sFlow Collector settings on page 18

- Configuring SNMP communication settings on page 19
- (Optional) Configuring email notifications on page 21

Enabling Host Tracker No Flood Hybrid Mode on the BSC Controller

Before you can successfully register devices with, or reconnect devices to the Brocade SDN Controller (BSC Controller), you must enable No Flood Hybrid Mode on the Controller. This is required to prevent ARP resolution failure.

ARP resolution failure occurs because by default, OpenFlow flows with an ARP match (all ARP packets) are automatically sent to the Controller, resulting in ARP resolution failure.

You can prevent ARP resolution failure by enabling No Flood Hybrid Mode on the Controller before you register devices with, or reconnect devices to the Controller.

> NOTE
> No Flood Hybrid Mode is part of the Controller's Host Tracker feature.

Pre-requisites: Make sure of the following:

- All of the required software is installed.
- You have access to the latest version of the *Brocade SDN Controller User Guide*. You use this guide to complete several steps of the procedure.

Complete these steps to enable No Flood Hybrid Mode on the Controller.

1. Enable No Flood Mode for the Host Tracker feature of the Brocade SDN Controller (refer to the *Brocade SDN Controller User Guide* for details).
2. Stop the controller (refer to the *Brocade SDN Controller User Guide* for details).
3. Enable Hybrid Mode for the ARP handler by doing the following:
    a) Navigate to the arp-handler file (`54-arphandler.xml`) in the controller server.

       The path is: `%CONTROLLER_INSTALLATION_FOLDER%/controller/etc/opendaylight/karaf/54-arphandler.xml`.

    b) Change the Hybrid Mode property setting (*<is-hybrid-mode></is-hybrid-mode>*) from False to True.
4. Start the Controller (refer to the *Brocade SDN Controller User Guide* for details).

Enabling Host Tracker No Flood Hybrid Mode on the ODL Controller

Before you can successfully register devices with, or reconnect devices to the OpenDayLight (ODL) Controller, you must disable Proactive Flood Mode and enable Hybrid Mode on the Controller. This is required to prevent ARP resolution failure.

ARP resolution failure occurs because by default, OpenFlow flows with an ARP match (all ARP packets) are automatically sent to the Controller, resulting in ARP resolution failure.

You can prevent ARP resolution failure by disabling Proactive Flood Mode and enabling Hybrid Mode on the Controller before you attempt to register devices with, or reconnect devices to the ODL Controller.

> NOTE
> Proactive Flood Mode and Hybrid Mode are part of the Controller's Host Tracker feature.

Pre-requisites: Make sure of the following:

- All of the required software is installed.

- You have access to the latest version of the *Open Day Light SR2 User Guide*. You use this guide to complete several steps of the procedure.

Complete these steps to disable Proactive Flood Mode and enable Hybrid Mode on the Controller.

1. Install ODL SR2 Lithium.

   The following packages need to be included (refer to the *Open Day Light SR2 User Guide* for details):

   - odl-restconf
   - odl-l2switch-hosttracker
2. Stop the Controller (refer to the *Open Day Light SR2 User Guide* for details).
3. Disable Proactive Flood Mode and enable Hybrid Mode for the ARP handler by doing the following:

   a) Navigate to the arp-handler file (`54-arphandler.xml`) in the Controller server.

      The path is: `%CONTROLLER_INSTALLATION_FOLDER%/controller/etc/opendaylight/karaf/54-arphandler.xml`.

   b) Change the Proactive Flood Mode property setting (*<is-proactive-flood-mode>/</is-proactive-flood-mode>*) from True to False.

   c) Change the Hybrid Mode property setting (*<is-hybrid-mode>/</is-hybrid-mode>*) from False to True.
4. Start the Controller (refer to the *Open Day Light SR2 User Guide* for details).

Enabling OpenFlow on MLX routers

Before you can begin using the Brocade Flow Optimizer application, you must enable OpenFlow on MLX routers. This involves specifying the OpenFlow Controller IP address and configuring various options for the maximum allowable number of OpenFlow entries.

The configuration OpenFlow entries enables you to set the maximum allowable OpenFlow entries for the following:

- The total number of OpenFlow entries.
- Protected and unprotected vlan entries.
- Layer 2 entries, layer 3 entries, and layer 2 and 3 entries.

Complete these steps to enable OpenFlow on MLX routers.

1. Telnet or SSH into the MLX router and get to the Configure Terminal mode.

   ```
   NetIron MLX-4 Router>enable
   NetIron MLX-4 Router#configure terminal
   NetIron MLX-4 Router(config)#
   ```

2. Enable OpenFlow Version 1.3 and configure the OpenFlow Controller IP address.
   The Controller IP address used in this example is 10.1.2.11.

   ```
   NetIron MLX-4 Router(config)#openflow enable ofv130
   NetIron MLX-4 Router(config)#openflow controller ip-address 10.1.2.11 no-ssl port 6653
   ```

3. Enable OpenFlow hybrid port mode on the interfaces.

   NOTE
   It is recommended that you specify Layer23 hybrid-mode.

   ```
   NetIron MLX-4 Router(config)#interface ethernet 1/1
   NetIron MLX-4 Router(config-if-e10000-1/1)#openflow enable layer23 hybrid-mode
   ```

4. Set the system maximum values. (system reload is required once you change the system maximum values).

   The system maximum values are as follows:

   - OpenFlow entries

     ```
     NetIron MLX-4 Router(config)#system-max  openflow-flow-entries <Valid Decimal Entry>
     DECIMAL   Valid range 0 to 65536 (default: 0)
     ```

   - OpenFlow protected VLAN entries

     ```
     NetIron MLX-4 Router(config)#system-max  openflow-pvlan-entries <Valid Decimal Entry>
     DECIMAL   Valid range 0 to 2048 (default: 0)
     ```

   - OpenFlow unprotected VLAN entries

     ```
     NetIron MLX-4 Router(config)#system-max  openflow-unprotectedvlan-entries  <Valid Decimal Entry>
     DECIMAL   Valid range 0 to 4096 (default: 0)
     ```

   - Max Np OpenFlow entries

     ```
     NetIron MLX-4 Router(config)#system-max np-openflow-entries layer2or3 | layer23IPv4 value slot
     [ i j k | i to z | all].
     ```

     (Slot number can be any of the valid slot number in the device. For slots, you can provide "all", "slot 1 to 2" and individual slot options.)

     One of the following parameters must be specified:

     – layer23IPv4: Layer 2 and 3, including L2 and IPv4 flow entries
     – layer23IPv6: Layer 2 and 3, including L2 and IPv6 flow entries

5. Reboot the system.

Enabling OpenFlow on ICX devices

Before you can begin using the Brocade Flow Optimizer application, you must enable OpenFlow on ICX devices. This involves specifying the OpenFlow Controller IP address and configuring various options for the maximum allowable number of OpenFlow entries.

When you enable OpenFlow, you also set the maximum allowable OpenFlow entries for the following:

- The total number of OpenFlow entries.
- Protected and unprotected vlan entries.

Complete these steps to enable OpenFlow on ICX devices.

1. Telnet or SSH into the router and get to the Configure Terminal mode.

   ```
   ICX Router>enable
   ICX Router#configure terminal
   ICX Router(config)#
   ```

2. Enable OpenFlow Version 1.3 and configure the OpenFlow Controller IP address.

   The Controller IP address used in this example is 10.1.2.11.

   ```
   ICX Router(config)#openflow enable ofv130
   ICX Router(config)#openflow controller ip-address 10.1.2.11 no-ssl port 6653
   ```

3. Enable OpenFlow hybrid port mode on the desired interfaces.

NOTE
It is recommended that you specify Layer23 hybrid-mode.

```
ICX Router(config)#interface ethernet 1/1/1
ICX Router(config-if-e10000-1/1/1)#openflow enable layer23 hybrid-mode
```

4. Set the system maximum values.

   A system reload is required after you change the system maximum values.

   The system maximum values are as follows:

   - OpenFlow entries

     ```
     ICX Router(config)#system-max openflow-flow-entries <Valid
     Decimal Entry>
     Decimal Valid range 0 to 12000 (default: 1024)
     ```

   - OpenFlow protected VLAN entries

     ```
     ICX Router(config)#system-max openflow-pvlan-entries <Valid
     Decimal Entry>
     Decimal Valid range 0 to 256 (default: 40)
     ```

   - OpenFlow unprotected VLAN entries

     ```
     ICX Router(config)#system-max openflow-unprotectedvlan-entries
     <Valid Decimal Entry>
     Decimal Valid range 0 to 256(default: 40)
     ```

5. Reboot the system.

Setting up the connection to the SDN Controller

You need to set up the connection to the SDN Controller to ensure that the Brocade Flow Optimizer is able to communicate with the Controller.

Before you set up the connection, check the following:

- Make sure that you have already enabled OpenFlow on your system devices (including ICX and MLX devices).
- If you want to set up HTTPS communication, make sure that HTTPS is turned on at the Controller. By default, HTTPS is turned off. Refer to the Controller manual for instructions.

  NOTE
  After you log in for the first time, you must set up the connection to the SDN Controller by entering the IP address of the Controller in the Brocade Flow Optimizer application. The only other time you need to enter the IP address of the Controller is if you change the configuration of your Controller and the IP address of the Controller has changed.

Complete these steps to complete the initial configuration of the Controller settings.

1. Go to the home directory for the application software distributable archive.
2. Open the `bin` folder.
3. Use one of the following commands to run the **startservice** script (this starts the application):
   - (Root user): **sh startservice**, or **./startservice**
   - (Non-root user): **sudo sh startservice**, or **sudo ./startservice**
4. Log in to the application.

   a) Open your browser and point it to the following URL:

https://<IP address of server>:8089

The port number must be 8089. This is the port number for the Brocade Flow Optimizer application.

A page appears with an alert that the connection may not be secure.

b) Select or click the option to continue with the connection.
The Login page appears.

c) Type your username and password and press **Enter**.

The **Dashboard** page appears.

5. Click **Settings** and then click the **General** tab.
6. Click **Add+** next to the SDN Controller Settings.

   The SDN Controller Settings dialog appears.
7. Optional: Select the **HTTPS** check box if you want secure communication with the Controller.

   By default, communication is over HTTP.
8. Enter the required SDN Controller information.
   - **IP Address** is the IP address of the Controller.
   - **Port** is the REST API port number of the Controller.
     - Enter 8443 if you selected the HTTPS check box.
     - Enter 8181 for HTTP connection.
   - **Username** and **Password** are the login credentials for the OpenFlow Controller.
9. Click **Save**.
   The Controller IP address and login credentials are saved in the system and are used for any REST calls made to the Controller by the application.

   NOTE
   If the application cannot connect to the Controller, a message displays indicating that the Controller is unreachable. This can be caused by any of the following:
   - Incorrect IP address or login credentials (username or password).
   - Incorrect REST API port number.
   - The Controller is not started (running).
   - A connectivity issue that is preventing the application from connecting to the Controller.

Enabling sFlow sampling of dropped packets on devices

If you want to use MLX devices, you must enable sFlow sampling of dropped packets on the devices.

NOTE
This task is not required for ICX 7750 and ICX 7450 devices. By default, sFlow sampling of dropped packets is enabled on the ICX 7750 and ICX 7450.

Complete these steps to enable sFlow sampling of dropped packets:

1. Telnet or SSH into the MLX router and get to the Configure Terminal mode.

```
NetIron MLX-4 Router>enable
NetIron MLX-4 Router#configure terminal
NetIron MLX-4 Router(config)#
```

2. Enter the following command to enable sFlow null0-sampling on the MLX device.

   ```
   MLX-4 router(config)# sflow null0-sampling
   ```

Configuring the sFlow Collector settings

Before you can begin monitoring flows, you must configure the sFlow Collector settings of the Brocade Flow Optimizer application. This task (along with configuring SNMP settings), is required to ensure that the Brocade Flow Optimizer server is able to receive sFlows.

Pre-requisites: Before you begin the procedure, make sure of the following:

- You have completed setting up the connection to the SDN Controller.
- You have enabled sFlow sampling of dropped packets for MLX devices. (For ICX7750 and ICX7450, it is enabled by default.)
- You know the correct In-band and Out-of-band addresses of Brocade Flow Optimizer server. This makes is easier to select the correct addresses, because the dialog you use to select the addresses lists all of the IP addresses currently configured on the host. It also helps to prevent sFlow registration from failure (selecting the wrong address for a device can cause the registration to fail).

  NOTE
  If the sFlow Collector settings are not configured or are incorrect, the Brocade Flow Optimizer server cannot receive the sFlows.

Configuring the sFlow Collector settings involves selecting the sFlow destination IP addresses for the devices. One IP address is named the In-band address, the other is named the Out-of-band address. You select the IP address based on the device type (ICX or MLXe).

- In-band address (MLXe devices only)
- Out-of-band (ICX devices only)

The system uses these IP addresses to register the sFlows for the devices. It uses the In-band address to register sFlows for MLXe devices, and the Out-of-band address to register sFlows for ICX devices.

Complete these steps to configure the sFlow Collector settings.

1. In the Brocade Flow Optimizer, go to the **Settings** page.
2. Click the **Devices** tab.
3. Click **+Add** next to sFlow Collector Settings.
   The **sFlow Collector Settings** dialog appears.
4. Do the following:
   a) Select the **In-band IP Address** (MLXe device).
   b) Select the **Out-of-band IP Address** (ICX device).
5. Click **Save**.
   The IP addresses are saved to the application database. The **sFlow Collector Settings** section of the **Devices** tab now shows the In-band IP Address and Out-of-band IP Address you selected.

Next steps: Configure the SNMP settings (this is required to complete the sFlow registration process).

Configuring SNMP communication settings

You must configure the SNMP settings before the sFlow registration process can be completed. The system uses SNMP for the communications between the Brocade Flow Optimizer server and system devices.

When you configure the SNMP settings, you define one or more SNMP profiles that are used by the system during the sFlow registration process. The SNMP profiles define the version of SNMP to be used and other SNMP options for the communications between the Brocade Flow Optimizer server and system devices.

As you define SNMP profiles, the system adds them in the order you define them to the list in the SNMP Settings section of the Devices tab. During the sFlow registration process, the system automatically selects an SNMP profile to use for the communication. The system starts with the first SNMP profile in the list of profiles you defined, and continues down the list until a suitable profile is found for the device. Once a suitable profile is found, the system automatically registers the sFlows. This process continues until all sFlows are registered for each device.

> NOTE
> If no suitable SNMP profile is found for a device, the sFlow registration fails, and an error message appears to let you know the registration could not be completed. If this occurs, modify the SNMP profiles you defined and repeat the registration process.

Types of SNMP profiles

There are two basic types of SNMP profiles. One type is based on v1 or v2 SNMP (this type is named v1/v2 SNMP profiles). The second type is based on v3 SNMP, and is named v3 SNMP profiles.

The profiles you define for the SNMP for the communications between the devices (ICX or MLX) and the Brocade Flow Optimizer server can be either v1/v2 SNMP profiles, or v3 SNMP profiles.

> NOTE
> You do not necessarily need to have both v1/v2 and v3 SNMP profiles. You can have only v1/v2 SNMP profiles, only v3 SNMP profiles, or a combination of v1/v2 and v3 profiles.

Defining the different profile types

The number and type of SNMP protocol options vary depending on the version of SNMP (v1/v2 or v3) you choose when you define the SNMP profiles. Because the SNMP options are the same for v1/v2 SNMP profiles, you use the same procedure to define v1/v2 SNMP profiles. You use a different procedure if you want to define v3 SNMP profiles.

Defining v1/v2 SNMP profiles

You must define one or more SNMP profiles before you can complete the sFlow registration process. The system uses the SNMP profiles for communications between the Collector and the Brocade Flow Optimizer server during the sFlow registration process.

Pre-requisites: Before you begin the procedure, make sure of the following:

- You have completed setting up the connection to the SDN Controller.
- You have completed setting up the sFlow Collector settings.

> NOTE
> If you want to use v3 SNMP for the communications involved in the sFlow registration process, do not use this procedure. Use the procedure for defining v3 SNMP profiles.

Complete these steps to define v1/v2 SNMP profiles.

1. Go to the **Settings** page.
2. Click the **Devices** tab.

3. Click **+Add** next to SNMP Settings.
   The **SNMP Settings** dialog appears.
4. Do the following:
   a) In the **Name** box, type a name for the profile. (For example, the network name or device name.)
   b) From the **Type** list, select **V1/V2**.
   c) Type the Read-Write community string.
5. Click **Save**.
   The profile is saved and is added to the list of profiles in the SNMP Settings section of the Devices tab.
6. (Optional) Repeat this procedure as needed to define additional v1/v2 SNMP profiles.

Next steps: You must register the system devices before they can be used to forward sFlow samples.

Defining v3 SNMP profiles

You must define one or more SNMP profiles before you can complete the sFlow registration process. The system uses the SNMP profiles for communications between the devices (ICX and MLX) and the Brocade Flow Optimizer server during the sFlow registration process.

Pre-requisites: Before you begin the procedure, make sure of the following:

- You have completed setting up the connection to the SDN Controller.
- You have completed setting up the sFlow Collector settings.

  NOTE
  If you want to use v1/v2 SNMP for the communications involved in the sFlow registration process, do not use this procedure. Use the procedure for defining v1/v2 SNMP profiles.

Complete these steps to define v3 SNMP profiles.

1. Go to the **Settings** page.
2. Click the **Devices** tab.
3. Click **+Add** next to **SNMP Settings**.
   The **SNMP Settings** dialog appears.
4. Fill out the fields in the dialog box.
   a) In the **Name** field, type a name for the profile. (For example, the network name or device name.)
   b) Select **V3** from the **Type** list.
   c) In the **User ID** field, type the User ID for the profile. (For example, the name of the group of users.)
   d) From the **Authentication Protocol** list, select the protocol to be used to encrypt the SNMP messages.
   e) In the **Authentication Password** field, type the authentication password. The correct password is required to enable the encryption of the SNMP messages.
   f) From the **Privacy Protocol** list, select the protocol to be used to make the SNMP messages private (only users with the right credentials can view the messages).
   g) In the **Privacy Password** field, type the privacy password. The correct password is required to enable the privacy of the SNMP messages.
5. Click **Save**.
   The profile is saved and is added to the list of profiles in the SNMP Settings section of the Devices tab.
6. Repeat steps 3 through 5 as needed to define additional v3 SNMP profiles.

Next steps: You must register the system devices before they can be used to forward sFlow samples.

Configuring email notifications

You can configure the Brocade Flow Optimizer to send automated email notifications to system users about events that affect traffic monitoring, so that they do not have to constantly monitor the system.

You must have Administrator privileges to set up or edit email notification settings.

Pre-requisites: Before you begin the procedure, make sure to have the following:

- SMTP port number and SMTP identifier (ID) for the email server (the server that sends the notifications to the specified set of system users).
- Reply address. This is the email ID (address) that sends the notifications to the specified set of system users.
- Email address of each user you want to set up to receive email notifications.

By default, the feature is not configured or enabled. You must configure the email notification options and enable the feature. You can enable or disable the notifications and edit the settings at any time.

Complete these steps to set up or edit the email notification settings.

1. In the Brocade Flow Optimizer, go to the **Settings** page and select the **General** tab.
2. Do one of the following based on whether you are setting up email notification for the first time, or editing your current setup:
   - **(Initial setup)**: In the **Email Settings** section, click **Add +**. The **Email Settings** dialog appears.
   - **(Edits)**: In the **Email Settings** section, click **Edit +**. The **Email Settings** dialog appears showing your current setup.
3. In the dialog, select the **Enable email notification** check box.
4. Specify the following:
   - **Email server** (Type the email address of the email server.)
   - **SMTP Port**
   - **SMTP ID**
   - **Password**
   - **Reply Address** (For example, no-reply@xyz.com).
   - **Email Address** (Type the email ID (email address) of each user you want to receive notifications. Be sure to separate the addresses using a comma.
5. (Optional) Test the email notification setup by doing the following:
   a) Type the email ID (email address) that you want to receive the test message (for example, your email address).
   b) Click **Send Test Email**.
   If the test email is sent to the specified address, a message appears in the dialog indicating the test was successful.
6. Click **Save** to save your email notification setup.

Email notification event types

All users that are set up to receive email notifications are automatically notified about events that affect traffic monitoring. All users set up to receive notifications receive notifications about the same types of events.

There are two basic types of events about which users can receive email notifications. They are as follows:

- Flow-related events. These are events about large flows (flows that exceed the threshold for the duration of the observation period).

- Profile-related events. These are events about the status of profiles (for example, a new profile has been created).

The following tables list and describe the flow-related events and profile-related events.

TABLE 3 Flow-related Events

Event	Description	Message
Large flow identified	The system has identified a large flow (a flow that has exceeded the Threshold value for the entire Observation Period defined in the profile associated with the flow). The message indicates the profile (by name) and the large flow (by the flow ID).	Large Flow identified for profile <profile name> • Profile definition The various large flow detection and mitigation action settings defined in the profile (for example, Threshold, Observation Time, and any network layer attributes). • Flow ID The unique identification number automatically assigned to the flow by the Brocade Flow Optimizer application.
Large flow mitigated	The system has applied the mitigation action to a flow that has been identified as a large flow. The mitigation action that has been applied is the action defined in the profile associated with the flow. The message indicates the profile (by name) and the large flow (by the flow ID). The Profile definition in the message also indicates the mitigation action that has been applied.	Large Flow mitigated for profile <profile name> • Profile definition The various large flow detection and mitigation action settings defined in the profile (for example, Threshold, Observation Time, and any network layer attributes). • Flow ID The unique identification number automatically assigned to the flow by the Brocade Flow Optimizer application.
Large flow blocked	The system has applied the Drop mitigation action to a flow that has already been identified as a large flow. The Drop mitigation action is defined in the profile associated with the flow. The message indicates the profile (by name) and the large flow (by the flow ID).	Large Flow deleted for profile <profile name> • Profile definition The various large flow detection and mitigation action settings defined in the profile (for example, Threshold, Observation Time, and any network layer attributes). • Flow ID The unique identification number automatically assigned to the flow by the Brocade Flow Optimizer application.

TABLE 4 Profile-related Events

Event	Description	Message
Profile added	A new profile has been created and is available for use. The new profile is in the list of profiles on the Profiles page. The message indicates the profile (by name) and gives the profile definition.	• Profile <profile name> added • Profile definition The various large flow detection and mitigation action settings defined in the profile (for example, Threshold, Observation Time, and any network layer attributes).
Profile edited	A profile has been edited and one or more profile parameters have been modified (for example, large flow detection parameters or the mitigation action has been modified). The message indicates the profile (by name) and gives the new profile definition.	• Profile <profile name> edited • Profile definition The various large flow detection and mitigation action settings defined in the profile (for example, Threshold, Observation Time, and any network layer attributes).

TABLE 4 Profile-related Events (continued)

Event	Description	Message
		The profile definition includes the new, modified parameter values.
Profile deleted NOTE When a profile is deleted, all flows being monitored using the profile are reset.	A profile has been deleted and is no longer available for use. The profile is no longer in the list of profiles on the Profiles page. The message indicates the profile (by name) and gives the profile definition.	• Profile <profile name> deleted • Profile definition The various large flow detection and mitigation action settings defined in the profile (for example, Threshold, Observation Time, and any network layer attributes).
Profile enabled	An existing profile has been enabled and is now available for use. The Profiles page shows the profile as enabled. The message indicates the profile (by name) and gives the profile definition.	• Profile <profile name> enabled • Profile definition The various large flow detection and mitigation action settings defined in the profile (for example, Threshold, Observation Time, and any network layer attributes).
Profile disabled NOTE If a profile is disabled when it is being used to monitor traffic, all flows being monitored using the profile are reset.	An existing profile has been disabled and is no longer available for use. The Profiles page shows the profile as disabled. The message indicates the profile by name and gives the profile definition.	• Profile <profile name> disabled • Profile definition The various large flow detection and mitigation action settings defined in the profile (for example, Threshold, Observation Time, and any network layer attributes).

Checking the application version

You can easily find which version of the Brocade Flow Optimizer you are using.

Complete these steps to find version information.

1. Login to the application.
2. On the Login page, click the **question mark** icon and choose **About**.
   The About dialog appears showing the version, build, and the time of installation.

Backing up the database

You can back up the database by running the database backup script (**dbbackup**). Running the script automatically triggers the database backup process. You do not need to stop the database server before you run the script.

The default backup type and target directory are as follows:

- backup-type: full
- target directory: SDN_HOME/backup/databases

You have the option of specifying a different target directory for the backup.

Complete these steps to back up the database:

1. Go to the home directory for the application software distributable archive.
2. Go to `bin` folder.

3. (Optional) Use the following command to open the Help so you can find the syntax to use the script:

   ```
   sh dbbackup --help
   ```

4. (Optional) Using the target-directory parameter of the **dbbackup** script, and specify the directory where you want the supportsave data saved.

   The directory name must not contain spaces. If you do not specify a directory, the default directory is automatically used (`SDN_HOME/backup/databases`).

5. Run the backup script (**dbbackup**).

   ```
   sh dbbackup
   ```

   The backup file is automatically saved to the target directory you specified, or to the default directory.

Restoring the database

You can restore the database by running the database restore script (**dbrestore**). Running the script automatically triggers the database restore process. You must stop the database server before you run the script.

Once you have completed the restore process, you need to restart the database. The following procedure provides the steps required to restore and restart the database.

1. Extract the distribution to one location (a single folder).
2. Run the **installdatabase** script.

   The script is included in the distribution you extracted in the previous step.

   This initializes the database server.

3. (Optional) Use the following command to open the Help so you can find the syntax to use the **dbrestore** script:

   ```
   sh dbrestore --help
   ```

4. Specify the name of the backup file you want to use to restore the database using the backup-file parameter of the **dbrestore** script.
5. Run the restore script, using the following command.

   ```
   sh dbrestore
   ```

   The database is restored using the data in the backup file.

6. Go to either of the following locations:
   - The target directory for the backup file used to restore the database.
   - The folder where the supportsave data is saved.
7. Copy the key value of the `security.pbe.key` file.
8. Go to the directory that contains the extracted distribution (see the first step of this procedure).
9. Replace the key value in the following files with the key value you copied from the `security.pbe.key` file:
   - `config.properties` file (replace the odl.controller.password value and the security.pbe.key value)
   - `database.properties` file (replace the database.password value)
10. Stop the database service using the following command:

    ```
    sh dbsvc stop
    ```

11. Run the **startservice** script to start the application.

Stopping the Brocade Flow Optimizer application

You can stop the Brocade Flow Optimizer application using just a few steps.

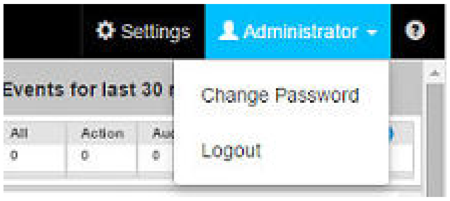
1. Go to the home directory (where the application files were installed).
2. Open the bin folder.
3. Use one of the following commands to run the **stopservice** script (this stops the application):
   - (Root user): **sh stopservice**, or **./stopservice**
   - (Non-root user): **sudo sh stopservice**, or **sudo ./stopservice**

   A message appears indicating that the application was stopped successfully.

Logging out

To end your current Brocade Flow Optimizer session, logout using the web client. The process is the same regardless of whether you have Administrator or Operator privileges.

1. Go to the Dashboard page.
2. Click on your username at the top-right of the page (next to the Settings tab), then choose **Logout**.

   The Dashboard page closes and the Login page appears.
3. (Optional) Close your browser.

Device Management

Modifying or re-entering the SDN Controller settings

The SDN Controller settings of the Brocade Flow Optimizer application must be modified or re-entered whenever the IP address of the Controller has changed or the Brocade Flow Optimizer application software is re-installed.

Complete these steps to modify or re-enter the Controller settings.

1. Click **Settings** and then click the **General** tab.
2. Click the **pencil icon** next to the SDN Controller Settings.
   The SDN Controller Settings dialog appears.
3. Modify or re-enter the SDN Controller Settings as needed.
   - **IP Address** is the IP address of the Controller.
   - **HTTPS** indicates whether you want secure (HTTPS) communication with the Controller. By default, communication is over HTTP.
   - **Port** is the REST API port number of the Controller.
     - Enter 8443 if you selected the HTTPS check box.
     - Enter 8181 for HTTP connection.
   - **Username** and **Password** are the login credentials for the OpenFlow Controller.
4. Click **Save**.
   The Controller IP address and login credentials are saved in the system and are used for any REST calls made to the Controller by the application.

   NOTE
   If the application cannot connect to the Controller, a message displays indicating that the Controller is unreachable. This can be caused by any of the following:

   - Incorrect IP address or login credentials (username or password).
   - Incorrect REST API port number.
   - The Controller is not started (running).
   - A connectivity issue that is preventing the application from connecting to the Controller.

Editing v1/v2 SNMP Profiles

You can easily edit existing SNMP profiles if the requirements change for SNMP communications between the Brocade Flow Optimizer server and system devices.

> NOTE
> You cannot edit the profile name.

Complete these steps to edit v1/v2 SNMP profiles.

1. Go to the **Settings** page.
2. Click the **Devices** tab.
3. In the list of SNMP profiles (SNMP Settings section), locate the profile you want to edit.
4. Click the **Edit** icon (pencil) in the Options column for the profile.
   The SNMP Settings dialog appears showing the current settings for the profile.
5. In the Read-Write community string box, edit the string.
6. Click **Save**.
   The changes are saved.
7. (Optional) Repeat steps 1 through 6 as needed to edit additional v1/v2 SNMP profiles.

Editing v3 SNMP Profiles

You can easily edit existing SNMP profiles if the requirements change for SNMP communications between the Brocade Flow Optimizer server and system devices.

> NOTE
> You cannot edit the profile name.

Complete these steps to edit v3 SNMP profiles.

1. Go to the **Settings** page.
2. Click the **Devices** tab.
3. In the list of SNMP profiles (SNMP Settings section), locate the profile you want to edit.
4. Click the **Edit** icon (pencil) in the Options column for the profile.
   The SNMP Settings dialog appears showing the current settings for the profile.
5. Do one or more of the following as needed:
   a) **User ID** Edit the User ID.
   b) **Authentication Protocol** Select the authentication protocol for the profile.
   c) **Authentication Password** Type the password for the authentication protocol.
   d) **Privacy Protocol** Select the privacy protocol for the profile.
   e) **Privacy Password** Type the password for the privacy protocol.
6. Click **Save**.
   The changes are saved.
7. (Optional) Repeat steps 1 through 6 as needed to edit additional v3 SNMP profiles.

How to read the list of registered devices

The list of devices in the Registered table in the Devices tab is the most current and reliable list of all of the system devices that are currently enabled to receive sFlow samples. You should be aware of how the list is updated by the system so that you can correctly interpret the meaning of the list.

The following table lists and describes the information in the Registered devices list.

Column	Description
Checkbox	The checkbox at the left side of the table is used to select devices when you want to unregister or delete the device. (Use the buttons in the Options column after you select the device.)
IP Address	The IP address of the device.
sFlow Enabled Port(s)	The list of ports on the device that are currently enabled for sFlow sampling (enabled to forward sFlow samples). This represents the port or ports that were selected when the device was registered. You can modify the list of ports by modifying the registration settings of the device.
Last Modified Time	The time of the latest (most recent): • Modification of device registration settings (such as the set of sFlow enabled ports or the sampling rate), **or** • Refresh of the list.
Last used SNMP	The name of the SNMP profile used during the latest successful registration of the device. NOTE If the SNMP profile that was used for the latest successful registration of the device has been deleted, this column is empty.
Options	This column provides buttons used to unregister a device, delete a device, and to edit the selection of sFlow enabled ports on the device. You edit the port selection by enabling or disabling sFlow forwarding on the device ports (checking a port enables sFlow forwarding, unchecking the ports disables sFlow forwarding). Select the device using the checkbox at the left side of the table.

Scenarios that can affect the listing of devices

You should be aware of how the list is updated by the system in certain scenarios so that you can correctly interpret the meaning of the list. There are steps you can take to ensure the lists are accurate.

Scenario	Steps for resolution
The SNMP communication fails for a device that was previously registered successfully. The SNMP communication failure is an unreachable or invalid SNMP profile. An error message appears, indicating that the SNMP profile is unreachable or invalid. This usually happens because: • The SNMP profile used for the latest successful registration has been deleted or edited. • The SNMP credentials have been modified on the device.	To retain the device and resolve the SNMP communication error, do one of the following: • Add the SNMP profile that was used for the latest successful registration. • Edit the existing SNMP profile so that it is valid for the device. NOTE If the device goes offline permanently, delete the device from the list to make sure the list is accurate.
A device that was previously registered successfully is no longer monitored by the Controller. This means that the device is no longer recognized by the Controller. An error message appears, indicating that the device is no longer monitored by the Controller.	In this case, you cannot re-register the device. Delete the device so that the Registered list is accurate.
After a refresh, the list of selected ports for the device is different from the ports that were selected during the latest successful registration of the device.	The database is automatically updated to show the new list of ports.

Scenario	Steps for resolution
The Brocade Flow Optimizer is no longer registered on a device as an sFlow destination. An error message appears, indicating that the application is no longer registered as an sFlow destination.	In this case, you cannot re-register the device. Delete the device from the Registered list to make sure the list is accurate.

Registering devices

Registering devices enables them to receive flows from the SDN Controller and forward sFlows to the Brocade Flow Optimizer application.

Pre-requisites: Before you can register a device, you must complete the initial system configuration to ensure that OpenFlow has been enabled on the device. You cannot register a device unless OpenFlow has been enabled on the device.

Device registration involves selecting the device or devices you want to register, and then selecting the ports on the device you want to be sFlow forwarding ports.

During the registration process, the system uses the SNMP profile (or profiles) you set up during the initial system configuration to configure the sFlow destination address on the device.

If a suitable SNMP profile is found, the Brocade Flow Optimizer application retrieves the current sFlow registration from the device, and the device is automatically added to the Manage list in the Devices tab. Any device listed in the Manage list can forward sFlows and be used to monitor traffic.

> NOTE
> Only devices that are listed in the list of Available devices in the Devices tab can be registered to forward sFlow samples. If a device is not currently listed in the Available section of the Devices tab, it cannot be registered.

> NOTE
> If a device is not currently listed in the Available section of the Devices tab, it cannot be registered.

Complete these steps to register a device.

1. In the Brocade Flow Optimizer, select the **Settings** page.
2. Click the **Devices** tab.
   The **Available** list in the tab shows all devices that are available for registration.
3. In the **Available** list, select the check box for the devices you want to register.

   The check box is grayed out if the device is already registered.
4. Click the **Register** link (in the **Options** column) for one of the devices you selected.
   If the registration was successful, the Register dialog appears showing a green checkmark next to the IP address of the device.
5. In the **Filter** box, type the IP address of the device. The address is used to filter on devices.
6. In the sFlow list, click the **checkbox** for each port you want to be a sFlow forwarding port. These ports will forward sFlows to the Brocade Flow Optimizer server.

   > NOTE
   > You must select at least one port. If you do not, the device cannot be registered.

7. Click **Apply**.
   The Register dialog closes.
8. Repeat steps **4** through **7** for the rest of the devices you selected to register.

The system uses the SNMP profile you set up during the initial system configuration to configure the sFlow destination address on the device. If a suitable SNMP profile is found, the Brocade Flow Optimizer application retrieves the current sFlow registration from the device, and the device is automatically added to the Manage list in the Devices tab. Any device listed in the Manage list can forward sFlows and be used to monitor traffic.

Unregistering devices

Unregistering a device disables the device from forwarding sFlow samples. Once the device is unregistered, it cannot forward sFlow samples to the Brocade Flow Optimizer server until it is registered again.

When you unregister a device, it is automatically moved to the list of devices that are available for registration. You use the **Devices** tab of the Settings page to unregister a device.

> NOTE
> If a device is not currently in the list of Registered devices in the **Devices** tab, it cannot be unregistered.

Complete these steps to unregister a device.

1. Select the **Settings** page.
2. Click the **Devices** tab.
   The **Registered** list in the tab shows all devices that are currently registered.
3. In the **Registered** list, click the checkbox for the device or devices you want to unregister.
4. Click the **Delete** link (in the Options column) for each device you selected to unregister.
5. Click the **Refresh** button to refresh the lists of Devices (the button is above the Register table).
   The lists of Devices are updated to reflect your changes.

Managing Registered Devices

Managing registered devices enables you to enable or disable sFlow on the ports of registered devices. Only ports on which sFlow has been enabled can forward sFlows to the Brocade Flow Optimizer server.

> NOTE
> This task applies only to devices that have been registered using the device registration process. All devices that are currently registered are listed in the Registered table of the Devices tab.

Complete these steps to enable or disable sFlow on the ports of registered devices.

1. Select the **Settings** page.
2. Click the **Devices** tab.
   The Registered list in the tab shows all devices that are currently registered to forward sFlow samples.
3. In the Registered list, click the **checkbox** for the devices you want to change the selection of sFlow enabled ports.
4. Click the **Manage** link (above the list of registered devices).
   The Register dialog appears showing the devices you selected.
5. In the sFlow list for a device, do the following:
   - Click the **checkbox** for each port you want to be an sFlow forwarding port. These ports are now enabled to forward sFlow samples.
   - Uncheck the **checkbox** for each port you do not want to be an sFlow forwarding port. These ports can no longer forward sFlow samples.

6. Repeat step **5** through for the rest of the devices you selected (if any).
7. Click **Apply**.
   The Register dialog closes.

Setting a device as a trigger for RTBH

Trigger devices are the devices that the Brocade Flow Optimizer uses to create static IP routes for the RTBH mitigation action.

A device must be BGP-enabled before it can be set as a trigger device.

Only MLX devices can be set as trigger devices.

1. In the Brocade Flow Optimizer, go to the **Settings** page.
2. Click the **Devices** tab.
3. In the **Registered** section, locate the device you want to use as a trigger.

   If the device you want is not listed in the **Registered** section, you must register it first.
4. Click the **pencil** icon in the **Set as Triggered** column, and provide the SSH login credentials.
5. Select the **For Trigger** check box next to the device you want to be the trigger.
6. Repeat the above steps for any other devices you want as trigger devices.

After you set up the trigger device, you can create a custom profile or user-defined flow to define the RTBH mitigation action.

Modifying the sFlow sampling rate of registered devices

The setting for the system sampling rate determines the rate at which ports forward sFlow samples. You can modify the sampling rate so that all currently registered devices forward sFlow samples at a rate other than the default.

The default sFlow sampling rate value for Brocade devices is 8192 (one packet out of every 8192 packets is sampled). The available sampling rate values are 8192, 16382, and 32768.

> NOTE
> The options for sampling rate vary depending on the device type.
>
> - **MLX** The sampling rate must be 8192 or 32768. MLX devices do not support the sampling rate of 16382. If you try to set the rate to 16382 on an MLX device, the system automatically sets it to 32768.
> - **ICX** ICX devices support all of the available sampling rates.

You modify the sampling rate by editing the Brocade Flow Optimizer configuration properties file (`config.properties`).

Complete these steps to modify the sampling rate for all devices that are currently registered.

1. Go to Brocade Flow Optimizer home directory (the directory where the application was installed).
2. Open the configuration folder, then open the configuration properties file (`config.properties`).
3. Locate the code used to specify the sampling rate.
   This example shows the default settings for a NetIron device.

```
sflow.samplingrate.netiron=8192
#sflow.samplingrate.netiron=16384
#sflow.samplingrate.netiron=32768
```

4. Modify the sampling rate by enabling the desired rate (un-comment the desired rate), and then comment out the rate you no longer want to use.

5. Save your changes and close the `config.properties` file.
6. Complete the following to ensure the changes take effect.
   a) Restart the Brocade Flow Optimizer server.
   b) Unregister all devices that are currently registered.
   c) Re-register all devices you unregistered in the previous step.

   The sampling rate is changed to the rate you specified.

User Management

Adding new users

The process for adding a new user involves specifying the name (username) and password for the user. Once the new user is added, they can use the Brocade Flow Optimizer application.

You must have Administrator privileges to add new users.

By default, all new users added by the Administrator have Operator privileges. Users with Operator privileges can do only the following:

- View the graphs and tables of real-time traffic monitoring data.
- View real-time events.
- Change their own password.

They cannot modify the system configuration, create or edit profiles, add or delete users, or change the passwords of other users.

Use the following procedure to add a new user.

1. In the Brocade Flow Optimizer, click the **Settings** button.
   The **Settings** page displays.
2. Click the **Users** tab.
   The list of current users appears.
3. Click the **+ Add User** link (above the list of users).
   The **Add New User** dialog appears.
4. Type the name (username) and password for the new user in the text boxes.
5. Click **OK**.
   The new user is added to the list of current users.

Changing user password

All users can change their own password. A user with Administrator privileges can also change the passwords of other users.

> NOTE
> If your system role is Operator (basic user) and the system Administrator changes your password while you are logged in, you are automatically logged out. To log in again, you must use your new password.

Complete these steps to change a user password:

1. Log in to the Brocade Flow Optimizer using your current credentials.
2. Go to the **Settings** page, and click the **Users** tab.

   The tab shows the list of current users.
3. Based on your user role (Administrator or Operator), do one of the following:
   - (Administrator) Click the **pencil** icon in the row of the user you want to edit.
   - (Operator) Click the **pencil** icon in the row of your user ID (your username).

The **Edit User** dialog appears.

4. Type the new password, then click **OK**.
   The user password is changed.

Deleting users

You can delete current users as part of your user management tasks. You must have Administrator privileges to delete users.

The process for deleting a user involves selecting the user and deleting them. Once the user is deleted, they cannot log in to use the Brocade Flow Optimizer application.

> NOTE
> If you delete a user while they are logged in, their session is interrupted and they are re-directed to the Login page. If they try to login, they are denied access.

Complete these steps to delete a user.

1. Click the **Settings** page.
2. Click the **Users** page.
   The list of current users appears.
3. Locate the user you want to delete, and click the **trash can** icon for the user (on the right side of the table).
   A message appears asking you to confirm that you want to delete the user.
4. Do one of the following:
   - Click **OK** to delete the user.
   - Click **Cancel** if you do not want to delete the user.

Profile Management

About profiles

Profiles are the main components of your traffic management policy enforcement. A profile is a configurable template you use to monitor a specific type of traffic.

The main purpose of a profile is to enable you to detect traffic that is above the bandwidth utilization threshold established in your traffic policy for that particular type of traffic.

Profiles also enable you to automate mitigation actions for any large flow that is detected. Once you configure the mitigation actions in the profile, the system automatically executes the actions on any large flow that is detected by the profile.

The Brocade Flow Optimizer provides two types of profiles for monitoring traffic.

- Default profiles
- Custom profiles

You configure profiles by setting parameters for the following:

- The network layer or layers at which traffic is inspected during traffic monitoring.
- The conditions that must be met for a flow to be identified as a large flow.
- The mitigation actions to be taken when a traffic flow is detected. The available mitigation actions vary depending on whether the profile is a default profile or a custom profile.

Default profiles

The Brocade Flow Optimizer provides seven default profiles for detecting volumetric traffic on your network. Use these profiles to detect and mitigate a variety of traffic that can consume network resources, disrupt the network, or degrade the general performance of the network.

You can enable, disable, and edit default profiles, and you can change the priority of default profiles.

NOTE
You cannot delete default profiles.

The default profiles are as follows:

- CharGen
- DNS Reflection
- ICMP Ping Flood
- NTP Reflection

- Quote of the Day
- Simple Service Discovery Protocol
- UDP Flood

CharGen

The CharGen profile monitors and detects potential malicious character generation protocol traffic listening on port 19, with UDP or TCP connections. This traffic is an attempt to consume network resources by causing devices to send high volumes of character generation traffic.

The mitigation actions available for this profile are Drop, Redirect, and None.

DNS Reflection

The DNS Reflection profile monitors and detects unrequested DNS query responses coming from third-party systems, (usually name servers). The third-party systems are responding to DNS queries sent from sources that typically cannot be traced.

Because the source IP address of the DNS queries is the IP address of the target, the target receives the DNS query responses. The traffic is amplified because the original DNS queries are often sent from multiple machines to numerous third-party systems. The result of the amplification is a huge amount of DNS query responses that consume the target network resources and disrupt the network.

The mitigation actions available for this profile are Drop, Redirect, and None.

ICMP Ping Flood

The ICMP Ping Flood profile monitors and detects ICMP echo requests (Ping packets) that did not originate in your network. The requests are a continuous series of Ping packets from sources that typically cannot be traced.

Because the source IP address of the ICMP echo requests is the IP address of the target, the target host receives the ICMP echo requests and responds with ICMP echo replies. The network becomes overloaded with the exchange of illegitimate ICMP echo and reply messages, which can result in a loss of transmission speed and general performance, and even connectivity issues.

The mitigation actions available for this profile are Drop, Redirect, and None.

NTP Reflection

The NTP Reflection profile monitors and detects unrequested responses from NTP servers. The NTP servers are responding to **get monlist** requests from sources that typically cannot be traced.

Because the source IP address of the **get monlist** requests is the IP address of the target, the target receives the responses from the servers. The traffic is amplified because the original **get monlist** requests are often sent from multiple machines to numerous NTP servers. The result of the amplification is a huge amount of **get monlist** responses that consume the target network resources and disrupt the network.

The mitigation actions available for this profile are Drop, Redirect, and None.

Quote of the Day

The Quote of the Day profile monitors and detects unsolicited requests to the Quote of the Day service. The traffic is amplified and results in a huge amount of requests to the connection or the datagram application listening on port 17.

The mitigation actions available for this profile are Drop, Redirect, and None.

Simple Service Discovery Protocol

The Simple Service Discovery Protocol profile monitors and detects unsolicited requests to Universal Plug and Play (UPnP) devices open to the Internet. The traffic is amplified and results in a huge amount of query responses that make the devices unresponsive.

The mitigation actions available for this profile are Drop, Redirect, and None.

UDP Flood

The UDP Flood profile monitors and detects illegitimate IP packets that contain UDP datagrams that are not associated with network applications.

Typically, the traffic is directed randomly at ports on the target host, which checks the network for applications associated with the UDP datagrams. Because no association exists, the target then responds with destination unreachable messages. The target host becomes overloaded with the exchange of illegitimate IP packets and destination unreachable replies, which prevents it from responding to other network clients.

The mitigation actions available for this profile are Drop, Redirect, and None.

Custom Profiles

The Brocade Flow Optimizer provides a highly configurable type of profile, called a custom profile, that you can use along with the default profiles to enforce your traffic management policy.

Like default profiles, custom profiles enable you to detect large flows and apply mitigation actions to those flows. Custom profiles use the traffic detection and mitigation action parameters used in default profiles.

Unlike default profiles, custom profiles support all of the available mitigation actions (None, Drop, Redirect, Remark, Meter, and Mirror). You can also specify network layer options, which are not available for default profiles.

You can create, enable, disable, edit, and delete custom profiles, and you can change the priority of custom profiles.

> NOTE
> You must have Administrator privileges to create, modify, or delete custom profiles.

The Brocade Flow Optimizer supports a maximum of 50 custom profiles. If you want to create additional custom profiles to monitor traffic, you must delete some existing custom profiles.

Mitigation parameters

Mitigation parameters are configurable profile parameters that determine the condition that must be met before traffic flows are identified as large flows.

The mitigation parameters are as follows:

- Observation time
- Threshold

If the bandwidth utilization of traffic targeted to a single destination exceeds the threshold value for the duration of the observation time, the flow is identified as a large flow, and the designated mitigation action is applied.

You configure the mitigation parameters when you create new custom profiles and when you edit custom or default profiles.

Mitigation actions

Mitigation actions are applied to flows that are identified as large flows. You can select from several mitigation actions to be applied to large flows.

The Brocade Flow Optimizer supports the following mitigation actions:

- None

  No mitigation action is taken. Use None to monitor flows without altering the traffic.
- Drop

  The flow is blocked. Sampling of sFlow traffic still occurs at the device ports even after the traffic is blocked.
- Redirect

  Traffic is redirected to one or more egress ports on a device you select to receive the traffic.
- Meter

  The traffic rate is limited (metered) to the bandwidth limitation you specify. This action is available only for custom profiles based on matching VLAN IDs.
- Mirror

  The flow is replicated and sent to a port you specify, called a mirror port. The original flow is unchanged. Select this action when you want to analyze a flow that is being received on an unprotected VLAN OpenFlow port (the ingress port). A typical use of this feature is performing deep packet analysis on one or more large traffic flows. This action is available only for custom profiles.
- RTBH (Remotely Triggered Black Hole)

  Drop traffic before it enters a protected network. Use RTBH to detect and mitigate DDOS attacks.

  > NOTE
  > The RTBH action is supported only on MLXe devices.

You configure the mitigation actions when you create new custom profiles and when you edit custom or default profiles.

Creating custom profiles

The Brocade Flow Optimizer enables you to create new profiles (called custom profiles) to use along with the default profiles to enforce your network management policy.

Pre-requisites: Make sure you are familiar with the large flow detection parameters and mitigation action parameters.

If you are using a NetIron device and you want to create a custom profile with the Mirror mitigation action, make that you do the following before you create the profile:

- Use the **acl-mirror-port** to configure the Mirror so that the ACL setting of the port matches the ACL setting on the ingress port (the port that receives the flow being monitored).

When you create a profile, you can specify up to three mitigation actions to create an end-to-end automated flow path for the traffic to reach third-party tools to further analyze the traffic.

Complete these steps to create a custom profile:

1. Go to the **Profile** page.
2. Click the **+Add Profile** link (near the top left of the page).
   The **Add Custom Profile** dialog appears.
3. In the **Profile Name** field, type the name for the profile.

The maximum length of the profile name is 128 characters. A profile name can contain only alphanumeric characters, spaces, and the following special characters: hyphen (-), period (.), underscore (_), and tilde (~).

4. In the **Description** field, type a description for the profile.
5. In the **Large flow detection settings** section, select one or more network layers (L2, L3, and L4) that are to be inspected during traffic monitoring.

   You can select any combination of layers, but you must select at least one layer.
6. For each layer you selected, enter the corresponding network attributes.
7. Configure the **Mitigation settings**.
   - **Observation Time (sec)** is the amount of time you want to monitor traffic before a flow is identified as a large flow.
   - **Threshold (Mbps)** is the bandwidth utilization threshold that a flow must exceed before it is identified as a large flow.
8. Select a mitigation action from the **Actions Settings** list.

   Depending on the action, a dialog box displays in which you must configure additional parameters.

   You can select up to three mitigation actions for a profile. If None or RTBH are selected, no other actions can be selected for that profile.
9. Click **Add** to close the **Add Custom Profile** dialog box.
   The profile is created and appears in the list of profiles on the Profile page.

Once the new custom profile is created, you can begin using it to monitor traffic.

Editing profiles

The Brocade Flow Optimizer enables you to edit profiles to ensure your current set of profiles can be used to effectively enforce your network traffic management policy.

You can edit both default and custom profiles. For custom profiles, you can edit the large flow detection settings and the mitigation settings. For default profiles, you can edit only the mitigation settings.

NOTE
You cannot change the name of the profile. If you want to change the name, you must delete the profile and re-create it using the new name.

1. In the Brocade Flow Optimizer, go to the **Profile** page.
2. Click the pencil icon next to the profile you want to edit.

   The pencil icon is in the **Options** column, on the right-hand slide of the page.

   The **Edit Profile** dialog box displays, populated with the current values for the profile.
3. In the **Description** field, enter or change the description.
4. In the **Large flow detection settings** section, select or clear the network layer check boxes (L2, L3, and L4).

   These settings determine which traffic layers are inspected during traffic monitoring. At least one layer must be selected.
5. For each layer you selected, enter or change the corresponding attributes.
6. Configure the **Mitigation settings**.
   - **Observation time (sec)** is the amount of time (in seconds) you want to monitor traffic before a flow is identified as a large flow.
   - **Threshold (Mbps)** is the bandwidth utilization threshold that a flow must exceed before it is identified as a large flow.
7. Configure the mitigation actions.

You may need to scroll down in the dialog box to see the **Actions Settings** section.

- Click the pencil icon to edit the action.
- Click the trash can icon to delete the action.
- Select additional actions from the **Add Action** list.

  You can configure up to three actions for the profile. If None or RTBH are selected, no other actions can be selected for that profile.

8. Click **Save** to close the **Edit Profile** dialog box and save your changes.
9. Verify your changes by clicking the arrow to the left of the profile name.
   An expanded view of the profile displays.

Deleting custom profiles

Deleting custom profiles enables you to remove profiles that are no longer used to enforce your traffic management policy.

> NOTE
> You cannot delete default profiles.

1. In the Brocade Flow Optimizer, go to the **Profile** page.
2. Use one of the following methods to delete custom profiles:
   - Click the trash can icon next to each custom profile you want to delete.

     The trash can icon is in the **Options** column, on the right-hand side of the page.
   - Select the check box next to each custom profile you want to delete, and click the **Delete** button above the table.

     Use this method if you want to delete several custom profiles at once.
3. Click **Yes** in the confirmation dialog box.

The profile is deleted. Any corresponding flows are removed from the SDN controller.

Changing the priority of a profile

Profile priority determines the order in which the Brocade Flow Optimizer validates currently defined profiles when sFlow samples are received. Changing the priority of profiles enables you to manage the order in which profiles are validated when monitoring traffic.

A priority is automatically assigned to a profile when you configure the profile. Default profiles are automatically assigned the highest priority, and custom profiles are automatically assigned the lowest priority.

The current priority ranking of the configured profiles is reflected in the list of profiles in the **Profile** page. Profiles are validated in the order they appear in the list. The profile at the top of the list has the highest priority.

> NOTE
> If the Brocade Flow Optimizer encounters a profile that matches the configuration of a profile with a higher priority that has already been validated, the lower priority profile is not validated.

1. In the Brocade Flow Optimizer, go to the **Profile** page.
2. Select the check box for each profile you want to change.

   You can select multiple profiles.
3. Click the Move buttons in the upper left-hand side of the page to move the selected profiles up or down in the list.

Moving profiles down the list decreases the priority. Moving profiles up the list increases the priority.

Enabling profiles

You must enable one or more profiles before the Brocade Flow Optimizer can monitor traffic to enforce your traffic management policy. For example, if you want to monitor NTP reflection traffic, you must enable an NTP Reflection profile.

On the **Profile** page, profiles that have a green checkmark are currently enabled. Profiles with a red no symbol are currently disabled.

1. In the Brocade Flow Optimizer, go to the **Profile** page.
2. Select the check box next to each profile you want to enable.

   You can select multiple profiles to enable.
3. Click the **Enable** button above the table.
   All of the selected profiles are now enabled. The red no symbol changes to a green checkmark.

Disabling profiles

Disable a profile if you want the Brocade Flow Optimizer to stop monitoring traffic based on that profile.

On the **Profile** page, profiles that have a green checkmark are currently enabled. Profiles with a red no symbol are currently disabled.

1. In the Brocade Flow Optimizer, go to the **Profile** page.
2. Select the check box next to each profile you want to disable.

   You can select multiple profiles to disable.
3. Click the **Disable** button above the table.
4. Click **Yes** in the confirmation dialog box.
   All of the selected profiles are now disabled. The green checkmark changes to a red no symbol.

Using Wildcards as Matching Criteria in Custom Profiles

Brocade Flow Optimizer supports the use of wildcards as matching criteria for network attributes in custom profiles. This enables you to define custom profiles that have a combination of highly specific and less specific matching criteria for network attributes.

Using wildcards is a very efficient way to detect flows that have a particular network attribute value. It eliminates or reduces the need to use numerous profiles to achieve the same detection capability. For example, if you want to detect all flows targeted to a particular VLAN, you can define a profile with the destination VLAN ID and use wildcards for the source MAC address and source IP address. This profile will detect all flows coming from any MAC address and IP address that have the same destination VLAN ID.

NOTE
The use of wildcards as matching criteria for custom profiles is limited to network attributes.

Maximum Number of Wildcards

There is no limitation on number of custom profiles that can have wildcards. However, a single custom profile cannot have more than 2 network attributes with wildcards as the matching criteria. If you select more than two wildcards for a profile, an error message appears when you click **Add** to create the profile.

Supported Mitigation Actions

Using wildcards is limited to custom profiles with the None mitigation action. If you try to specify a mitigation action other than None, an error message appears when you click **Add** to create the profile.

Format Requirements for Specifying Wildcards

When specifying wildcards for network attributes, you must use the correct format to ensure the wildcard is accepted. The formatting requirements for wildcards vary depending on whether the wildcard is an address (MAC or IP address), or an integer value.

The guidelines for specifying wildcards are:

- **MAC addresses** You can specify a wildcard for the entire MAC address (for example, *), or for one or more of the tuples in the address (for example, FF : * : GG : * : * : *).
- **Integers** You can specify a wildcard for any network attribute that takes a single integer value, a range of values, or comma-separated values.
- **IP addresses** You can specify a wildcard for the entire IP address (for example, *) or specify a subnet range for the IP address.

The following table lists the formatting requirements for each of the network attributes that can accept wildcards.

Examples of Matching Results

The following examples show the expected matching behavior when using wildcards in custom profiles.

Example 1: Source MAC address

In this example, a wildcard is specified for the source MAC address. A range of values is specified for the VLAN ID. The specified matching criteria are:

- **Source MAC address** `AA: * : DD : * : * : *`
- **Destination VLAN ID** `10-20`

The following table lists the expected matches for a custom profile containing these matching criteria.

Matching MAC Addresses	Matching VLAN IDs
AA:CC:DD:AA:DD:1E	Any vlan ID between 10 and 20 (inclusive)
AA:D2:DD:A2:C3:1F	
Non-matching MAC Addresses	Non-matching VLAN IDs
CC :C1:DD:A3:4F:DD	Any VLAN ID below 10 and greater than 20
AA:2D: **FF** :A4:34:AC	

Example 2: Source MAC address and Destination VLAN ID

In this example, wildcards are specified for the entire source MAC address and the destination VLAN ID. The specified VLAN Priority value is 5. The specified matching criteria are:

- **Source MAC address** `*`
- **Destination VLAN ID** `*`
- **VLAN Priority** `5`

When using these matching criteria, all flows with a source MAC address, a destination VLAN ID, and a VLAN Priority value of 5 will match.

Example 3: Source IP address

In this example, a wildcard is specified for the source IP address. The specified VLAN Priority value is 5. The specified matching criteria are:

- Source IP address `*`
- VLAN Priority `5`

When using these matching criteria, all flows initiated from unique SRC IP (*.*.*.*/32) that have a VLAN Priority value of 5 will match.

Validation of Matches Against Wildcards

Validations for wildcard matches are performed on the client and at the REST API layer.

Flow Management

Flow terminology

Before you begin using the tabs of the Flows page, make sure you become familiar with the basic terms used to categorize the different types of flows. The terms are also the names of the tabs used to list the different flows.

Learned and Programmed Flows

Learned and Programmed flows are all the traffic flows received by the Brocade Flow Optimizer server that meet the following criteria:

- Have been identified as large flows (flows that have exceeded the bandwidth threshold and observation period of a current, active profile). The flows are 'learned' because the flow is known by the Brocade Flow Optimizer.
- The system has applied the mitigation action to the flow that is specified in the profile associated with the flow.
- The flow is programmed because a mitigation action based OpenFlow rules has been automatically programmed on the device through the use of profiles.
- For the mitigation action "None", no action or OpenFlow rule is programmed on the device.

NOTE
Although the Current Large Flows table in the Dashboard page lists the same type of flow, it lists only the 50 flows that are consuming the most bandwidth. The Learned and Programmed Flows table lists all of flows (including the flows shown in the Current Large Flows table).

Learned Flows

Learned flows are all the traffic flows received by the Brocade Flow Optimizer server that meet the following criteria:

- Have not been identified as large flows (the flows have not exceeded the bandwidth threshold and observation period of any of the current, active profiles). The flows are 'learned' because the flow is known by the Brocade Flow Optimizer.
- The system has not applied any mitigation action to the flow (because the large flow detection criteria have not been met).
- The flow is not programmed. The flow may not be monitored by a specific profile and it has not exceeded the bandwidth threshold. As a result, no OpenFlow rule for the flow is programmed on the device through the use of profiles.

NOTE
Learned flows can be flows that are being monitored using profiles as well as flows that are not being monitored using profiles. By listing both types of flows, the system enables you to discover flows that you may not be aware of and apply a mitigation action to the flow to optimize network bandwidth.

User Defined Flows

User-defined flows are all the flows created by Brocade Flow Optimizer administrators. These are custom flows created using the available network attributes or parameters and mitigation actions.

User-defined flows include the following:

- Flows created from learned flows using options provided in the **Learned Flows** tab.
- Flows created by adding new flows using the Add Custom Flow option (click the **Create Flow** button to access the Add Custom Flow option).

Discovering large flows using filter criteria

Use the filter (search) criteria in the **Learned and Programmed Flows** tab to discover large flows that cannot be viewed using other system components.

When you select filter (search) criteria, follow these rules:

- To search (filter) on an item, specify a value for the item (for example, a MAC address), or select an item using the pick-list for the item.
- You must select at least one item to filter the results.
- You can select as many items as you want to include in your search.
- Items you do not select by specifying or selecting a value are not used to filter the results.
- Before you run the search, clear the filters to ensure that only the filter terms you want to use are used in your search.

Complete these steps to discover large flows using filter criteria.

1. Select the **Flows** page, then click the **Learned & Programmed Flows** tab.
2. Click **Refresh** to view the latest set of active large flows.
3. Click **Clear** to remove any filters from the previous search.
4. In the **Filter** section, enter values for the items on which you want to filter.
5. Click the **Search** option (it is at the top right of the tab).
   The flows that match the filter criteria you selected are shown in the table below the filter options.

Discovering large flows by inspecting flows in the list

Use the **Learned and Programmed Flows** tab to see if a large flow is a composite flow comprised of one or more large flows. This enables you to discover large flows that are contained within another large flow that cannot be viewed using other system components.

Complete these steps to discover large flows by inspecting other flows.

1. In the Brocade Flow Optimizer, go to the **Flows** page, then click the **Learned & Programmed Flows** tab.
2. Click **Refresh** to view the latest set of active large flows.
3. Scan the list of flows to find a flow you want to inspect.
4. Click the **View** option for the flow (it is at the right side of the list).
   The detailed information for the selected flow are shown in the table.

   NOTE
   If the selected flow is comprised of multiple flows, all of the flows are listed in the table.

If you determine you want to monitor any of the flows using a profile, you can create a new profile for that purpose.

Discovering Learned Flows using filter criteria

Use the filter (search) criteria in the **Learned Flows** tab to discover learned flows that cannot be viewed using other system components.

When you select filter (search) criteria, follow these rules:

- To search (filter) on an item, specify a value for the item (for example, a MAC address), or select an item using the pick-list for the item.
- You must select at least one item to filter the results.
- You can select as many items as you want to include in your search.
- Items you do not select by specifying or selecting a value are not used to filter the results.
- Before you run the search, clear the filters to ensure that only the filter terms you want to use are used in your search.

Complete these steps to discover learned flows using filter criteria.

1. Select the **Flows** page, then click the **Learned Flows** tab.
2. Click **Refresh** to view the latest set of active learned flows.
3. Click **Clear** to remove any filters from the previous search.
4. In the Filter section, enter values for the items on which you want to filter.

   In the **Name** field, you can enter all or part of the flow name.
5. Click the **Search** option (it is at the top right of the tab).
   The flows that match the filter criteria you selected are shown in the table below the filter options.
6. Scan the list of flows.

   NOTE
   If you find a flow that you want manage, you can create a custom flow based on the flow in the list. Complete the remaining steps to create a custom flow.
7. (Optional) To create a custom flow from a flow in the list, click the **Apply** option for the flow (at the right end of the table).
   The flow is automatically added to the **User Defined Flows** tab.

Creating custom flows from learned flows

The Brocade Flow Optimizer enables you to create custom (user-defined) flows from learned flows. Once you create the custom flow, you can monitor the flow in the same way that flows are monitored using profiles.

A user-defined flow is a flow that you use to monitor flows on the network. When you create a user-defined flow, you define the network attributes (including MAC addresses, IP addresses, ports, IP protocols, VLAN ID, and mitigation action) you want to use as the matching criteria for the flow.

NOTE
(Optional) If you want to filter the list of learned flows before creating a custom flow, complete the procedure.

Complete these steps to create a new flow from a learned flow.

1. Select the **Flows** page, then click the **Learned Flows** tab.
2. Click **Refresh** to view the latest set of active learned flows.
3. (Optional) If you want to filter the list of learned flows before creating a custom flow, select the search criteria you want to use, then click the **Search** option. (It is at the top right of the tab).
   The flows that match the filter criteria you selected are shown in the table below the filter options.
4. Click the **Apply** option for the flow you want to use to create the custom flow. (The **Apply** option is at the right end of the table).

The flow is automatically added to the **User Defined Flows** tab.

Creating user-defined flows

User-defined flows are custom flows that you create using the available network attributes and mitigation actions.

Make sure you are familiar with the large flow detection parameters and mitigation action parameters.

When you create a flow, you can specify up to three mitigation actions to create an end-to-end automated flow path for the traffic to reach third-party tools to further analyze the traffic.

Complete these steps to create a user-defined flow.

1. In the Brocade Flow Optimizer, go to the **Flows** page, and click the **User Defined Flows** tab.
2. Click the **Create Flow** link.
   The **Add Custom Flow** dialog appears.
3. In the **Flow Name** field, type the name for the flow.

   The maximum length of the profile name is 128 characters. A profile name can contain only alphanumeric characters, spaces, and the following special characters: hyphen (-), period (.), underscore (_), and tilde (~).
4. In the **Action Settings** list, select a mitigation action.

   Depending on the action, a dialog box displays in which you must configure additional parameters.

   You can select up to three mitigation actions for a flow. If None or RTBH are selected, no other actions can be selected for that profile.
5. In the **Large flow detection settings** section, select one or more network layers (L2, L3, and L4) that are to be inspected during traffic monitoring.

   You can select any combination of layers, but you must select at least one layer.

   The L2 and L4 check boxes are inactive when RTBH is the mitigation action.
6. For each layer you selected, enter the corresponding network attributes.
7. Select a priority for the flow.
8. Click **Add** to close the **Add Custom Flow** dialog box.
   The flow is created and appears in the list of flows in the **User Defined Flows** tab.

Discovering user-defined flows using filter criteria

Use the filter (search) criteria in the **User Defined Flows** tab to discover user-defined (custom) flows that cannot be viewed using other system components.

When you select filter (search) criteria, follow these rules:

- To search (filter) on an item, specify a value for the item (for example, a MAC address).
- You must select at least one item to filter the results.
- You can select as many items as you want to include in your search.
- Items you do not select by specifying or selecting a value are not used to filter the results.
- Before you run the search, clear the filters to ensure that only the filter terms you want to use are used in your search.

Complete these steps to discover user-defined flows using filter criteria.

1. Select the **Flows** page, then click the **User Defined Flows** tab.

2. Click **Refresh** to view the latest set of active large flows.
3. Click **Clear** to remove any filters from the previous search.
4. In the **Filter** section, enter values for the items on which you want to filter.

   In the **Name** field, you can enter all or part of the flow name.
5. Click the **Search** option (it is at the top right of the tab).
   The flows that match the filter criteria you selected are shown in the table below the filter options.

Deleting user-defined flows

If flows are inactive, you should delete them, to improve the Brocade Flow Optimizer performance.

> NOTE
> You cannot deleted Learned flows or Learned and Programmed flows.

1. In the Brocade Flow Optimizer, go to the **Flows** page.
2. Click the **User Defined Flows** tab.
3. Use one of the following methods to delete user-defined flows:
   - Click the trash can icon next to each user-defined flow you want to delete.

     The trash can icon is in the **Options** column, on the right-hand side of the page.
   - Select the check box next to each user-defined flow you want to delete, and click the **Delete** button above the table.

     Use this method if you want to delete several user-defined flows at once.
4. Click **Yes** in the confirmation dialog box.

The selected flows are deleted.

Changing the inactive time limit for large flows

For improved performance, inactive flows are automatically deleted from the database. For large flows, you can configure the amount of time the flow can be inactive before it is automatically deleted from the database.

By default, large flows are automatically deleted from the database if the large flow is inactive for more than one day. You can configure this inactive time to be one day, one week, or 30 days.

Learned flows that are not part of Large flows are automatically deleted from the database if the Learned flow is inactive for more than one hour. This time is not configurable.

You modify the inactive time limit by editing the Brocade Flow Optimizer configuration properties file (`config.properties`).

1. Go to Brocade Flow Optimizer home directory (the directory where the application was installed).
2. Open the configuration folder, then open the configuration properties file (`config.properties`).
3. Locate the code used to specify the large flow inactive limit.

   ```
   largeflow.inactive.limit=1d
   ```
4. Modify the limit by specifying the time limit you want.

   The supported time limit values are as follows:
   - 1d (one day)
   - 1w (one week)

- 30d (30 days)

The following example automatically deletes large flows if they are inactive for more than one week.

```
largeflow.inactive.limit=1w
```

5. Save your changes and close the `config.properties` file.
6. Restart the Brocade Flow Optimizer server.

Real-time Events

The Brocade Flow Optimizer provides records two types of real-time events. One type is traffic monitoring events and the other type is audit events. Every event logged by the application has a time stamp, description, and a unique identifier.

Both types of real-time events can be viewed on the Events page, or the Events pane of the Dashboard. The Events page lists events that have occurred over the last few days or more. The Events pane of the Dashboard lists events that have occurred over the last 30 minutes.

The application stores a maximum of 50000 events. Any events beyond the maximum storage capacity are purged nightly from the database.

The different real-time events are:

- Controller Settings Added: Indicates that sFlow Controller settings have been configured. This typically indicates the post-installation configuration that is done as part of the initial system configuration.
- Controller Settings Updated: Indicates that sFlow Controller settings have been updated (modified). This indicates a change to the existing configuration.
- Flow Added: Indicates that the flow was successfully added to the profile. The profile name appears in the description of the event.
- Flow Creation Failed: The flow that was configured and enabled for monitoring could not be generated.
- Flow Detected: Indicates that the flow has been detected as a large flow, which means that the flow has exceeded the bandwidth utilization threshold for the flow. The yellow warning icon appears on the left side next to the event.
- Flow Removed: Indicates that the flow was successfully removed. Flows are removed if the bandwidth utilization falls below the bandwidth utilization threshold.
- Flow Removal Failed: A flow that was detected and should have been removed based on the specified mitigation action could not be removed.
- Meter Created: A meter was set up in the system for a flow based on your configuration settings.
- Meter Deleted: A meter was set up in the system for a flow based on your configuration settings was successfully deleted.
- Meter Add / Delete Failed: A meter that you set up for a flow could not be created, or a meter that you selected for deletion could not be deleted.
- Mitigated: A flow that was detected has been mitigated based on the mitigation action you specified for the flow. The different mitigation actions are:
  - Default profiles: The mitigation action events are Drop, Redirect, and None.
  - Custom profiles: The mitigation action events are Drop, Redirect, None, Remark, and Meter.
- Profile Created: A profile you configured has been created by the system.
- Profile Deleted: A profile you deleted from your set of profiles (policy) has been successfully removed from the system.
- Profile Add / Delete Failed: A profile that you configured could not be created, or a profile that you selected for deletion could not be deleted.
- Audit: The total number of events performed by users (Administrator or Operator) that have been logged during the last 30 minutes of the current session. This includes the changing of controller settings, adding, editing, or deleting profiles, and user management events.

Web Client

Dashboard page

The Dashboard page is the landing page of the Brocade Flow Optimizer application. It is the page you use to get a snapshot of the current traffic being monitored, including the traffic profiles that have the highest current bandwidth utilization (as Mbps). You also use it to view graphs of real-time traffic monitoring data and the most recent real-time events.

When you login, the Dashboard page appears showing the Overall Traffic Rate graph, the Current Large Flows tables (shown below the Overall Traffic Rate graph), and the Events pane. The Overall Traffic Rate graph and Current Large Flows tables show traffic monitoring data, and the Events section shows events for the last 30 minutes.

NOTE
To view a full history of events, use the Events page.

Overall Traffic Rate

The Overall Traffic Rate graph provides a real-time snapshot of the traffic currently being monitored by the application. All of the flows currently being monitored using profiles are represented in the graph.

The graph is a stacked graph that shows two very basic types of traffic: traffic that is being blocked, and traffic that is being passed through the system. This graph shows data for last 30 minutes and is refreshed once every 60 seconds. The graph continues plotting data if the window is minimized or goes out of focus.

The x-axis shows the time stamp (on the application Client), and the y-axis shows the throughput in Mbps. The blocked traffic and passed traffic are represented in the graph using different colors, and each traffic type is shown in its own stack in the graph. The legend indicates the colors used to represent the block traffic and passed traffic.

The meaning of blocked and passed traffic are as follows:

Blocked Traffic	Large traffic flows (in Mbps) that are being blocked. The traffic is being blocked because the bandwidth utilization of the flows has exceeded the bandwidth utilization threshold, and the Drop mitigation action is being applied to the flows.
Passed Traffic	Large traffic flows (in Mbps) that are not being blocked. The traffic is being redirected, remarked, metered, or allowed to pass unaltered because the bandwidth utilization of the flows has exceeded the bandwidth utilization threshold for the flows, and the selected mitigation action is being applied to the flows. The mitigation action you have selected in the profile determines whether the flow is being re-directed, remarked, metered, or allowed to pass unaltered.

Blocked Traffic details

To view details about the blocked traffic, click the **Blocked Traffic** link at the top-right of the graph. The **Large Flow (Blocked Traffic) - Detailed View** dialog appears.

The dialog shows large flows (flows that exceed profile thresholds) that are being dropped. The mitigation actions defined in the profiles used to monitor the traffic are actions that result in the traffic being dropped.

By default, the dialog shows the 5 large flows (blocked traffic) that have the highest bandwidth utilization (as Mbps) for the most recent 30 minutes. The graph is refreshed once every 15 seconds. Each flow is represented in the graph using a different color. The table below the graph lists the details (such as source and destination ports), for each of the flows in the graph.

To view historical data for blocked traffic, click one of the following labels at the top-right of the Large Flow (Blocked Traffic) - Detailed View dialog:

- **1h:** View data for the last hour.
- **1d:** View data for the last day.
- **1w:** View data for the last week.
- **30d:** View data for the 30 days.

The following table lists the columns in the Large Flow (Blocked Traffic) - Detailed View dialog.

Source IP	The IP address of the source interface of the flow.
Destination IP	The IP address of the destination interface of the flow.
Source MAC	The MAC address of the source interface of the flow.
Destination MAC	The MAC address of the destination interface of the flow.
Source Port	The port number of the source port of the flow.
Destination Port	The port number of the destination port of the flow.
VLAN	The VLAN to which the flow belongs. This is the VLAN ID. If the flow does not belong to a VLAN, this column is empty.
Traffic (Mbps)	The bandwidth utilization of the flow (as Mbps).

Passed Traffic details

To view details about the passed traffic, click the **Passed Traffic** link at the top-right of the graph. The Large Flow (Passed Traffic) - Detailed View dialog appears.

The dialog shows large flows (flows that exceed profile thresholds) that are not being dropped. The mitigation actions defined in the profiles used to monitor the traffic are not actions that result in the traffic being dropped.

By default, the dialog shows the 5 large flows (passed traffic) that have the highest bandwidth utilization (as Mbps) for the most recent 30 minutes. The graph is updated once every 15 seconds. Each flow is represented in the graph using a different color. The table below the graph lists the details (such as source and destination ports), for each of the flows in the graph.

To view historical data for passed traffic, click one of the following labels at the top-right of the Large Flow (Passed Traffic) - Detailed View dialog:

- **1h:** View data for the last hour.
- **1d:** View data for the last day.
- **1w:** View data for the last week.
- **30d:** View data for the 30 days.

The columns in the Large Flow (Passed Traffic) - Detailed View dialog are the same as for the Large Flow (Blocked Traffic).

Current Large Flows

The Dashboard provides lists of flows that have been identified as large flows (flows that have exceeded the specified bandwidth utilization). Two lists are provided in the Dashboard: one for flows being monitored by Default profiles, and one list for flows being monitored by Custom profiles. Each list is presented in its own table.

The data is real-time data, and is refreshed every 15 seconds. The title of each table indicates whether the list is for flows being monitored using Default profiles or Custom profiles. If none of the flows being monitored exceed the bandwidth utilization threshold for the duration of the observation period, no large flow is detected and the table is empty. (This applies to both the Default Profiles table and the Custom Profiles table.)

> NOTE
> Each table lists the large flows that have the highest bandwidth utilization (as Mbps). The maximum number of flows that can be listed in the Current Large Flows tables is 50.

To view all of the flows, click the **View All** link at the top right corner of the table. You are re-directed to a Flows tab, which shows all of the flows.

Current Large Flows table for Default profiles

This table lists the flows being monitored using Default profiles that have the highest bandwidth utilization. To view a real-time graph of the flow, click the blue flow icon at the left side of the table.

The columns in this table are:

- **Link to real-time graph** To view a real-time graph of the flow, click the blue flow icon at the left side of the table.
- **Traffic (Mbps):** The bandwidth utilization of the flow as Mbps.
- **Identified On:** The time stamp (on the application client) when the flow was detected.
- **Destination:** The destination IP address of the flow.
- **Profile Name:** The name of the profile. (You cannot define or modify the name of Default profiles.)
- **Action:** The mitigation action specified in the profile used to monitor this flow.

Current Large Flows table for Custom profiles

This table lists the flows being monitored using Custom profiles that have the highest bandwidth utilization. To view a real-time graph of the flow, click the blue flow icon at the left side of the table.

The columns in this table are:

- **Traffic (Mbps):** The bandwidth utilization of the flow as Mbps.
- **Identified On:** The time stamp (on the application client) when the flow was detected.
- **L2:** The layer 2 large flow detection parameters defined in the profile.
  - SRC MAC: The source MAC address.
  - DEST MAC: The destination MAC address.
  - SRC VLAN: The VLAN ID of the ingress port.
  - 802.1q: The VLAN priority.
- **L3:** The layer 3 large flow detection parameters defined in the profile.
  - Source IP V4: IPV4 source IP address.
  - Destination IP V4: IPV4 destination IP address.
  - Source IP V6: IPV6 source IP address.
  - Destination IP V6: IPV6 destination IP address.

  - IP protocol: The IP protocol (TCP, UDP, or ICMP).
  - DSCP: Di_ Serv Code Point (part of the IPv4). ToS field or the IPv6 Traffic Class field.
  - IP Fragment: Yes / No
- L4: The layer 4 large flow detection parameters defined in the profile.
  - TCP SRC PORT: TCP source port.
  - TCP DST PORT: TCP destination port.
  - UDP SRC PORT: UDP source port.
  - UDP DST PORT: UDP destination port.
  - TCP Flags: TCP Flags (SYN, FIN, ACK, RST, URG, or PSH).
- Profile Name: The name of the profile.
- Action: The mitigation action specified in the profile used to monitor this flow.

Events pane

The Events pane of the Dashboard lists the real-time traffic monitoring events and auditing events that have occurred within the last 30 minutes. The table is automatically updated every 15 seconds with the most recent real-time events.

> NOTE
> If you want to view events that have occurred over the last few days or more, use the Events page (click on the **Events** tab of the Dashboard).

You can scroll through the list to view more events. If you get to the bottom of the list, use the buttons on the bottom of the pane to view the next page of events.

For each event, the following information is provided in the columns of the Events pane:

- Severity The icon at the left of each entry indicates the severity of the event.

⊗	Critical event
⚠	Warning event
ℹ	Information event (system-wide events that occur during the processing of flows and application of mitigation actions)

- Message ID The unique identifier for the message. (Shown next to the severity icon.)
- Time The time the event occurred (the client time stamp).
- Description A brief description of the event.

The Events page also provides counters for real-time events.

All	The total number of events that have been logged during the last 30 of the current session.
Action	The total number of events related to monitoring traffic for large flows. These events include the setup of profiles, flows, the detection of large flows, the execution of mitigation actions and more.
Audit	The total number of events performed by users (Administrator or Operator) that have been logged during the last 30 minutes of the current session. This includes the changing of controller settings, adding, editing, or deleting profiles, and user management events.

Flows Page

The Flows page enables you to discover and view all of the flows (openflows) on the network, including flows that are being monitored using profiles, and flows that are not being monitored using profiles or being manipulated or processed in any way by the system. It also enables you to easily view all of the custom flows you create from existing flows you have discovered.

The Flows page contains the following three tabs:

- Learned & Programmed Flows
- Learned Flows
- User Defined Flows

You use the tabs of the Flows page for two main purposes. One is to discover flows that cannot be viewed using other components of the application. The other purpose is to create your own OpenFlow flows (called user-defined flows) from flows you have discovered.

Discovering flows

The Flows page provides functionality you use to discover flows that cannot be viewed using other components of the application. This helps you to have better insight about the network flows and gives you the opportunity to manage the flows you discover.

You use the Learned and Programmed Flows tab and the Learned Flows tab to discover flows. The two basic methods you use to discover flows are:

- Viewing flows (without filtering).
- Filtering (searching) for flows using filter criteria.

Learned and Programmed Flows tab

This tab lists of all of the large flows received by the Brocade Flow Optimizer server. You use this tab to discover large flows that are not listed in other system components.

The search filter options are in the top half of the tab. The list of large flows is provided in a table below the search filter options.

List of flows

The flows are listed from top to bottom based on the bandwidth utilization, with the greatest bandwidth utilization at the top of the table. The table provides the same information about the large flows that is provided in the **Current Large Flows** table of the Dashboard, with the exception of the OpenFlow statistics.

📈	Opens the real-time graph for the flow.
Traffic (Mbps)	The amount of bandwidth consumed by the flow.
Identified on	The time that the flow was identified as a large flow. This represents when the system recognized that the flow exceeds the large flow detection criteria defined in the profile used to monitor the flow.
L2 / L3 / L4	The network layer attributes of the flow. The values for each attribute (L2, L3, or L4) are listed in separate columns.
Profile	The name of the profile associated with the flow.
Action	The mitigation actions defined in the profile that is associated with the flow. Up to three actions can be defined.
Details	Click **View** to display OpenFlow statistics for each mitigation action. • **Byte Count** is the number of bytes in the flow that have been mitigated. • **Packet Count** is the number of packets in the flow that have been mitigated.

If the number of flows is greater than 50, use the pagination options to navigate through the list of flows.

Learned Flows tab

This tab lists all of the traffic flows learned from sFlows received by the Brocade Flow Optimizer server.

Use the **Learned Flows** tab to discover flows that have not been detected as large flows that are not listed in other system components. You can also use this tab to create custom flows from the discovered flows.

Learned flows can be the following:

- Flows that are being monitored using profiles, but have not exceeded the large flow detection criteria of the profile associated with the flow.
- Flows on the network that are not being monitored using profiles.

By default, this tab shows the active learned flows for the past 30 minutes. This page is not automatically refreshed. Click **Refresh** to view the latest set of learned flows.

The search filter options are in the top half of the tab. The list of learned flows is provided in a table below the search filter options.

Filter options

You can filter the list of flows displayed by entering values in the **Filter** section. For example, you can display only the flows from a specific IP address, or only the flows having a specific name.

Enter values for the fields you want to search on. Leaving a field blank means that the criteria is not used to filter the results. For example, if you enter a flow name and leave all other fields blank, then all flows that match the name are displayed, regardless of the IP or MAC addresses, or any other parameter values.

Field / Component	Description
Traffic (Mbps)	Select whether to display all traffic, or traffic that is greater than or less than a specific Mbps value. If you select **Greater than** or **Less than**, enter the number of Mbps in the adjacent field.
Name	The name of the flow. Enter all or part of the name you want to search for.
Source MAC	The source MAC address.
Destination MAC	The destination MAC address.
Ingress VLAN ID	The ingress VLAN ID.
Source IP	The source IP address.
Destination IP	The destination IP address.
IP Protocol	Select the IP protocol from the list. Selecting **ALL** includes all IP protocols in the search.
Source Port	The source port number.
Destination Port	The destination port number.

Click **Search** to display a filtered list of flows, based on the criteria you specify.

Click **Clear** to clear all of the filter fields.

List of flows

The flows are listed from top to bottom based on the bandwidth utilization, with the greatest bandwidth utilization at the top of the table.

In addition to the standard parameters, you can display additional MPLS, VXLAN, and IPSec parameters by selecting the corresponding check boxes at the top of the table.

If the number of flows is greater than 50, use the pagination options to navigate through the list of flows.

Field / Component	Description
Show check boxes: - MPLS - VXLAN - IPSEC	Select one or more check box to display additional information about the flow. MPLS and VXLAN are applicable only to NetIron (MLX) platforms. IPSEC is applicable to both NetIron (MLX) and FastIron (ICX) platforms.
Refresh	Click to refresh the list of flows displayed.
Name column	Click the field and type a new name for the flow.
Action column	Click **Apply** in the **Action** column to change any of the other values for the flow.

User Defined Flows tab

This tab lists all of the current custom (user-defined) flows. Use this tab to discover user-defined flows that are not listed in other system components, and to create custom flows.

This page is not automatically refreshed. Click **Refresh** to view the latest set of user-defined flows.

The search filter options are in the top half of the page. The list of learned flows is provided in a table below the search filter options.

Filter options

You can filter the list of flows displayed by entering values in the **Filter** section. For example, you can display only the flows from a specific IP address, or only the flows having a specific name.

Enter values for the fields you want to search on. Leaving a field blank means that the criteria is not used to filter the results. For example, if you enter a flow name and leave all other fields blank, then all flows that match the name are displayed, regardless of the IP or MAC addresses, or any other parameter values.

Field / Component	Description
Name	The name of the flow. Enter all or part of the name you want to search for.
Source MAC Destination MAC	The source and destination MAC addresses.
Ingress VLAN ID	The ingress VLAN ID.
VLAN Priority	For a tagged VLAN, the 802.1p VLAN priority. The VLAN priority is a number between 0 and 7, inclusive.
Source IP Destination IP	The source and destination IP addresses.
IP Protocol	Select the IP protocol from the list. Selecting **ALL** includes all IP protocols in the search.
DSCP	The Differentiated Services Code Point (DSCP) value. The DSCP value is a number between 0 and 63, inclusive.
Source Port Destination Port	The source and destination port numbers.

Click **Search** to display a filtered list of flows, based on the criteria you specify.

Click **Clear** to clear all of the filter fields.

List of flows

The flows are listed from top to bottom based on the bandwidth utilization, with the greatest bandwidth utilization at the top of the table. If the number of flows is greater than 50, use the pagination options to navigate through the list of flows.

In the **Options** column, click the **trash can** icon to delete the flow. You can select the check boxes next to the flows and click **Delete** to delete several flows at one time.

Click **Details** to display additional information about the flow. The View Flow Details dialog box displays OpenFlow statistics for each mitigation action.

- **Byte Count** is the number of bytes in the flow that have been mitigated.
- **Packet Count** is the number of packets in the flow that have been mitigated.

Add Custom Flow dialog

Use the **Add Custom Flow** dialog to create new custom flows.

Fields and components

TABLE 5 Fields and components of Add Custom Flow dialog box

Field/Component	Description
Flow Name field	The name of the flow. The maximum length of the flow name is 128 characters. A flow name can contain only alphanumeric characters, spaces, and the following special characters: hyphen (-), period (.), underscore (_), and tilde (~). You can use the same name for multiple flows. For example, you can give all flows going to the same data center the same name. If you leave this field blank, then the flow name becomes the same as the flow ID. NOTE Use care when selecting a name. Once the flow is created, you cannot update the name.
Detection settings	A set of configurable parameters that determine which traffic layers are inspected during traffic monitoring.
Layer 2 configuration parameters	
L2 check box	Indicates that Layer 2 traffic is to be inspected during traffic monitoring. Selecting this check box displays additional Layer 2 parameters that are to be configured.
Source MAC field **Destination MAC** field	The source and destination MAC addresses. The MAC address is specified in 6-tuples, separated by colons (:), for example: 12:73:51:22:79:99. You can optionally include a mask at the end of the MAC address. The mask format must be 6-tuples of either "ff" or "00". For example, the MAC entry 11:22:33:44:55:66/ff:ff:00:00:00:00 matches all MAC addresses that start with "11:22". You can also use wildcards in the MAC address.
Ether Type field	A decimal value that indicates which protocol is encapsulated in the Ethernet frame payload. **Ether Type** cannot be a negative value. It is your responsibility to provide valid values to identify flows. Note the following restrictions: • If you select **L3** and provide an IPv4 source or destination IP address, then **Ether Type** must be set to 2048 (for IPv4). • If you select **L3** and provide an IPv6 source or destination IP address, then **Ether Type** must be set to 34525 (for IPv6).
VLAN check box	Indicates that a VLAN is to be monitored. Selecting this check box displays additional VLAN parameters that are to be configured.
Tagged and **Untagged** options	Indicates whether the VLAN is a tagged VLAN or an untagged VLAN.
Ingress VLAN ID field	For a tagged VLAN, the ID of the ingress VLAN.
VLAN Priority field	For a tagged VLAN, the 802.1p VLAN priority. The VLAN priority is a number between 0 and 7, inclusive.
Layer 3 configuration parameters	
L3 check box	Indicates that Layer 3 traffic is to be inspected during traffic monitoring. Selecting this check box displays additional Layer 3 parameters that are to be configured.

TABLE 5 Fields and components of Add Custom Flow dialog box (continued)

Field/Component	Description
IP Type list	Select IPV4 or IPV6.
Source IP field **Destination IP** field	The source and destination IP addresses, in CIDR notation. Enter an IPv4 address or an IPv6 address, depending on the IP Type you selected.
IP Protocol list	The IP protocol for the flow.
DSCP field	The Differentiated Services Code Point (DSCP) value. The DSCP value is a number between 0 and 63, inclusive.
Layer 4 configuration parameters	
L4 check box	Indicates that Layer 4 traffic is to be inspected during traffic monitoring. Selecting this check box displays additional Layer 4 parameters that are to be configured.
Source Port field **Destination Port** field	The source and destination port numbers.
Priority settings options	These options determine the priority of the flows and actions. Select **High** if you want the priority to be higher than learned and programmed flows. Select **Low** if you want the priority to be lower than learned and programmed flows.
Action Settings list	The action automatically applied to flows that have been identified as large flows. Select from the following options: • Drop • Redirect • Meter • Mirror • RTBH (Remotely Triggered Black Hole) Selecting an action displays a dialog box in which additional parameters must be configured. You can select up to three actions, for example, if you want to create an end-to-end open flow path to redirect the traffic to third party analyzers. If you select RTBH, you cannot select any other actions. The RTBH action is supported only on MLXe devices.
Action tables	Configuration information about the selected actions is displayed at the bottom of the dialog box. You can edit or delete the action by clicking the **pencil** or the **trash can** icons, respectively.

BGP Settings dialog (for flows)

Use the BGP Settings dialog to specify a tag value for the route, for RTBH mitigation actions.

The BGP Settings dialog contains the following fields:

Field / Component	Description
Tag field	Specifies the tag value of the route to use for route filtering with a route map. Valid values range from 0 through 4294967295. The default is 0.

Profile page

The Profile page lists all of the Default profiles and Custom profiles that are available for use. The Profile page provides an easy-to-read view of the current profiles, including the current bandwidth consumed by the flows being monitored by the profile.

In addition to viewing the list of current profiles and profile details, you use this page to:

- View basic information about a profile, such as the name, large flow detection parameters, and mitigation action.
- View detailed information about a profile (click the arrow button next to the profile name).

- Enable, disable, or delete profiles.
- Open the dialogs used to create new Custom profiles or to edit existing profiles.
- Change the priority of a profile.

For each profile, the following information is provided on the Profile page:

- Status (enabled or disabled): A green checkmark icon indicates the profile is enabled and is being used to monitor traffic flows. A red checkmark icon indicates the profile is disabled and is being used.
- Profile name: The name of the profile. For default profiles, this is pre-defined and cannot be changed. For custom profiles, this is the name specified when the profile was created or when it was edited.
- Observation Time: The amount of time (in seconds) that the application monitors the bandwidth utilization of traffic targeted to a single destination before marking it as a large flow. If the bandwidth utilization exceeds the Threshold value for the duration of the Observation time, the flow is identified as a large flow.
- Threshold: The bandwidth utilization threshold (in Mbps) used to identify a flow as a large flow. If the bandwidth utilization of a flow exceeds the value throughout the Observation time, the flow is marked as a large flow.
- Action: The mitigation action defined in the profile (for example, Drop, Redirect, Mirror, or Meter).
- Last Modified By: The username of the person that was the last user to modify the profile.
- Last Modified Time: The timestamp of the last modification made to the profile.
- Options: The available options for the profile. For Default profiles, you can only edit the profile. For Custom profiles, you can edit or delete the profile.

Viewing profile details

You can view the details for a profile by clicking the arrow next to the name of the profile. When you click on the arrow, the page shows the expanded view for the profile. The expanded view shows all of the options and specified values for the profile.

NOTE
You cannot use the expanded view to edit the profile. It is a read-only view of the profile.

For more information on profiles, see the following:

- About profiles on page 37
- Custom Profiles on page 39
- Default profiles on page 37
- Edit Profile dialog on page 69
- Enabling profiles on page 43
- Disabling profiles on page 43
- Editing profiles on page 41

Add Custom Profile dialog

Use the **Add Custom Profile** dialog to create new custom profiles.

Fields and components

Field/Component	Description
Profile Name field	The name of the profile. The maximum length of the profile name is 128 characters. A profile name can contain only alphanumeric characters, spaces, and the following special characters: hyphen (-), period (.), underscore (_), and tilde (~).
Description field	A brief description of the profile. The maximum length of the description is 512 characters.
Large flow detection settings	A set of configurable parameters that determine which traffic layers are inspected during traffic monitoring.
Mitigation settings	A set of configurable parameters that determine the conditions that must be met before traffic flows are identified as large flows.
Actions Settings	A set of configurable parameters that determine the mitigation action taken on large flows.

Large flow detection settings

The large flow detection settings are a set of configurable parameters that determine which traffic layers are inspected during traffic monitoring. As you select the L2, L3, and L4 check boxes, additional parameters are displayed that you must configure.

Field/Component	Description
Layer 2 configuration parameters	
L2 check box	Indicates that Layer 2 traffic is to be inspected during traffic monitoring. Selecting this check box displays additional Layer 2 parameters that are to be configured.
Source MAC field **Destination MAC** field	The source and destination MAC addresses. The MAC address is specified in 6-tuples, separated by colons (:), for example: 12:73:51:22:79:99. You can optionally include a mask at the end of the MAC address. The mask format must be 6-tuples of either "ff" or "00". For example, the MAC entry 11:22:33:44:55:66/ff:ff:00:00:00:00 matches all MAC addresses that start with "11:22". You can also use wildcards in the MAC address.
Ether Type field	A decimal value that indicates which protocol is encapsulated in the Ethernet frame payload. **Ether Type** cannot be a negative value. It is your responsibility to provide valid values to identify flows. Note the following restrictions: • If you select **L3** and provide an IPv4 source or destination IP address, then **Ether Type** must be set to 2048 (for IPv4). • If you select **L3** and provide an IPv6 source or destination IP address, then **Ether Type** must be set to 34525 (for IPv6).
VLAN check box	Indicates that a VLAN is to be monitored. Selecting this check box displays additional VLAN parameters that are to be configured.
Tagged and **Untagged** options	Indicates whether the VLAN is a tagged VLAN or an untagged VLAN.
Ingress VLAN ID field	For a tagged VLAN, the ID of the ingress VLAN.
VLAN Priority field	For a tagged VLAN, the 802.1p VLAN priority. The VLAN priority is a number between 0 and 7, inclusive.
Layer 3 configuration parameters	
L3 check box	Indicates that Layer 3 traffic is to be inspected during traffic monitoring. Selecting this check box displays additional Layer 3 parameters that are to be configured.
Source IP (IPv4) field **Destination IP (IPv4)** field	The source and destination IPv4 addresses, in CIDR notation.
Source IP (IPv6) field **Destination IP (IPv6)** field	The source and destination IPv6 addresses, in CIDR notation.

Field/Component	Description
IP Protocol list	The IP protocol for the flow.
DSCP field	The Differentiated Services Code Point (DSCP) value. The DSCP value is a number between 0 and 63, inclusive.
IP Fragment list	If you select **Yes** or **No**, the mitigation action is automatically set to None and cannot be changed.
Layer 4 configuration parameters	
L4 check box	Indicates that Layer 4 traffic is to be inspected during traffic monitoring. Selecting this check box displays additional Layer 4 parameters that are to be configured.
TCP Source Port field **TCP Destination Port** field	The TCP source and destination port numbers. If you specify TCP port numbers, you cannot also specify UDP port numbers.
UDP Source Port field **UDP Destination Port** field	The UDP source and destination port numbers. If you specify UDP port numbers, you cannot also specify TCP port numbers.
TCP Flags list	A list of supported TCP flags. If selected, only traffic with the matching TCP flag is inspected. Note that if you select a TCP flag, the mitigation action is automatically set to None and cannot be changed.

Mitigation settings

Mitigation settings are a set of configurable parameters that determine the conditions that must be met before traffic flows are identified as large flows.

Field/Component	Description
Observation Time (sec) field	The amount of time (in seconds) that the Brocade Flow Optimizer monitors the bandwidth utilization of traffic targeted to a single destination before marking it as a large flow. If the bandwidth utilization exceeds the Threshold value for the duration of the Observation Time, the flow is identified as a large flow. NOTE When the bandwidth utilization of traffic that has been identified as a large flow falls below the Threshold value for the duration of the Observation Time, the traffic is no longer identified as a large flow.
Threshold (Mbps) field	The bandwidth utilization threshold (in Mbps) used to identify a flow as a large flow. If the bandwidth utilization of a flow exceeds the value throughout the Observation Time, the flow is marked as a large flow.

Action Settings

Action settings are a set of configurable parameters that determine the mitigation action taken on large flows.

Field/Component	Description
Action list	The action automatically applied to flows that have been identified as large flows. Select from the following options: • None • Drop • Redirect • Meter • Mirror • RTBH Selecting an action displays additional parameters that must be configured. You can select up to three actions, for example, if you want to create an end-to-end open flow path to redirect the traffic to third party analyzers.

Field/Component	Description
	If you select None or RTBH (Remote Trigger Black Hole), you cannot select any other actions. If you select RTBH, you can specify only L3 large flow detection settings. Any L2 or L4 settings are automatically cleared.
Action tables	Configuration information about the selected actions is displayed at the bottom of the dialog box. You can edit or delete the action by clicking the **pencil** or the **trash can** icons, respectively.

Node Ports Picker dialog

Use the **Node Ports Picker** dialog when adding or editing profiles, to select devices and ports for the profile.

The content of the **Node Ports Picker** dialog differs, depending on the mitigation action.

Node Ports Picker dialog for Drop action

If the mitigation action is Drop, select the ingress ports in the Node Ports Picker dialog.

TABLE 6 Fields and components of the Node Ports Picker dialog box when action is Drop

Field/Component	Description
Nodes check boxes	If you select no nodes and no ports, then the drop action is applied to all registered devices. If you select one or more nodes, and no ports, then the drop action is applied to the generic flows on those nodes. If you select one or more ports, then the drop action is applied to the port-specific flows.
Match changes	If you previously specified a destination MAC or an ingress VLAN, you can remove the original criteria or you can override the match criteria with different values. If **Remove** and **Override** are grayed out, it means no destination MAC or ingress VLAN ID was previously specified.

Node Ports Picker dialog for Meter action

If the mitigation action is Meter, you select the ingress ports and, optionally, the rate limit and DSCP configuration.

TABLE 7 Fields and components of the Node Ports Picker dialog box when action is Meter

Field/Component	Description
Rate Limit (Mbps) field	The bandwidth utilization rate (in Mbps) used to limit the flow. The rate of the flow is limited to the value you specify. All the traffic above the rate limit is dropped, unless you select the **DSCP Remark** check box. This field is available only for the Meter action.
DSCP Remark check box	Select this check box to decrease the drop-precedence of the DSCP field in the IP header of the packet, for traffic above the rate limit. If this check box is not selected, if traffic is above the rate limit (specified in the **Rate Limit (Mbps)** field), the traffic is dropped. If this check box is selected, if traffic is above the rate limit, the DSCP field in the IP header of the packet is set to the value in the **DSCP Precedence** field. This parameter is available only for the Meter action.
DSCP Rate Limit (Mbps) field	The maximum bandwidth utilization for the DSCP remark.
DSCP Precedence field	The value that the drop-precedence field in the IP header is set to, if the traffic is above the rate limit.
Nodes check boxes	Select the check box for the ingress port. The selected port and the corresponding node are displayed in the table.

Node Ports Picker dialog for Mirror action

If the mitigation action is Mirror, you select the ingress port and mirror port.

TABLE 8 Fields and components of the Node Ports Picker dialog box when action is Mirror

Field/Component	Description
Nodes options	Select the node for the mirror action.
Ingress port list	Select the ingress port from this list.
Mirror port list	Select the mirror port from this list. The mirror port and the ingress port cannot be the same.

Node Ports Picker dialog for Redirect action

If the mitigation action is Redirect, you select the ingress and egress ports, destination MAC, and VLAN ID and action.

TABLE 9 Fields and components of the Node Ports Picker dialog box when action is Redirect

Field/Component	Description
Nodes list	Select the node. The nodes are listed by IP address.
Ingress and **Egress** check boxes	Select the **Ingress** and **Egress** check boxes corresponding to the ingress and egress ports. The selected ports and corresponding node are displayed in the table. You must select at least one egress port. You can select multiple egress ports per node. The ingress port is optional.
Destination MAC field	Destination MAC address in 6-tuples, separated by : (colon).
VLAN Action option buttons	Select from the following actions: • **None** • **Push**: The VLAN ID you specify in this dialog box is pushed onto the ingress packet and forwarded to the egress port. • **Pop**: The VLAN ID in the ingress packet is stripped and sent out to the egress port. Select the **Pop** option for traffic flowing from tagged to untagged devices. • **Modify**: If the ingress packet is tagged with a VLAN ID, the VLAN ID you specify in this dialog box overrides the VLAN ID in the ingress packet. The traffic sent to the egress port has the VLAN ID you specify here. Select the **Modify** option for traffic flowing between devices of different VLANs. If you select **Push** or **Modify**, you must also enter the **VLAN ID**.
VLAN ID field	The VLAN ID to be sent out to the egress port, if the VLAN action is Push or Modify.
Match changes	If you previously specified a destination MAC or an ingress VLAN, you can remove the original criteria or you can override the match criteria with different values. If **Remove** and **Override** are grayed out, it means no destination MAC or ingress VLAN ID was previously specified.

BGP Settings dialog (for profiles)

Use the BGP Settings dialog to specify a tag value and prefix length for the route, for RTBH mitigation actions.

The BGP Settings dialog contains the following fields:

Field / Component	Description
Tag field	Specifies the tag value of the route to use for route filtering with a route map. Valid values range from 0 through 4294967295.
Prefix Length field	Specifies the BGP prefix length. Valid values range from 1 through 32.

Edit Profile dialog

Use the **Edit Profile** dialog to edit existing profiles. You can edit both default and custom profiles.

Fields and components

Field/Component	Description
Profile Name field	The name of the profile. You cannot edit this field. If you want to change the name, you must delete this profile and re-create it using a different name.
Description field	A brief description of the profile. The maximum length of the description is 512 characters.
Large flow detection settings	A set of configurable parameters that determine which traffic layers are inspected during traffic monitoring.
Mitigation settings	A set of configurable parameters that determine the conditions that must be met before traffic flows are identified as large flows.
Actions Settings	A set of configurable parameters that determine the mitigation action taken on large flows.

Large flow detection settings

The large flow detection settings are a set of configurable parameters that determine which traffic layers are inspected during traffic monitoring. As you select the L2, L3, and L4 check boxes, additional parameters are displayed that you must configure.

Field/Component	Description
Layer 2 configuration parameters	
L2 check box	Indicates that Layer 2 traffic is to be inspected during traffic monitoring. Selecting this check box displays additional Layer 2 parameters that are to be configured.
Source MAC field **Destination MAC** field	The source and destination MAC addresses. The MAC address is specified in 6-tuples, separated by colons (:), for example: 12:73:51:22:79:99. You can optionally include a mask at the end of the MAC address. The mask format must be 6-tuples of either "ff" or "00". For example, the MAC entry 11:22:33:44:55:66/ff:ff:00:00:00:00 matches all MAC addresses that start with "11:22". You can also use wildcards in the MAC address.
Ether Type field	A decimal value that indicates which protocol is encapsulated in the Ethernet frame payload. **Ether Type** cannot be a negative value. It is your responsibility to provide valid values to identify flows. Note the following restrictions: • If you select **L3** and provide an IPv4 source or destination IP address, then **Ether Type** must be set to 2048 (for IPv4). • If you select **L3** and provide an IPv6 source or destination IP address, then **Ether Type** must be set to 34525 (for IPv6).
VLAN check box	Indicates that a VLAN is to be monitored. Selecting this check box displays additional VLAN parameters that are to be configured.
Tagged and **Untagged** options	Indicates whether the VLAN is a tagged VLAN or an untagged VLAN.
Ingress VLAN ID field	For a tagged VLAN, the ID of the ingress VLAN.
VLAN Priority field	For a tagged VLAN, the 802.1p VLAN priority. The VLAN priority is a number between 0 and 7, inclusive.
Layer 3 configuration parameters	
L3 check box	Indicates that Layer 3 traffic is to be inspected during traffic monitoring. Selecting this check box displays additional Layer 3 parameters that are to be configured.
Source IP (IPv4) field **Destination IP (IPv4)** field	The source and destination IPv4 addresses, in CIDR notation.
Source IP (IPv6) field **Destination IP (IPv6)** field	The source and destination IPv6 addresses, in CIDR notation.
IP Protocol list	The IP protocol for the flow.

Field/Component	Description
DSCP field	The Differentiated Services Code Point (DSCP) value. The DSCP value is a number between 0 and 63, inclusive.
IP Fragment list	If you select **Yes** or **No**, the mitigation action is automatically set to None and cannot be changed.
Layer 4 configuration parameters	
L4 check box	Indicates that Layer 4 traffic is to be inspected during traffic monitoring. Selecting this check box displays additional Layer 4 parameters that are to be configured.
TCP Source Port field **TCP Destination Port** field	The TCP source and destination port numbers. If you specify TCP port numbers, you cannot also specify UDP port numbers.
UDP Source Port field **UDP Destination Port** field	The UDP source and destination port numbers. If you specify UDP port numbers, you cannot also specify TCP port numbers.
TCP Flags list	If selected, only traffic with the matching TCP flag is inspected. Note that if you select a TCP flag, the mitigation action is automatically set to None and cannot be changed.

Mitigation settings

Mitigation settings are a set of configurable parameters that determine the conditions that must be met before traffic flows are identified as large flows.

Field/Component	Description
Observation Time (sec) field	The amount of time (in seconds) that the Brocade Flow Optimizer monitors the bandwidth utilization of traffic targeted to a single destination before marking it as a large flow. If the bandwidth utilization exceeds the Threshold value for the duration of the Observation Time, the flow is identified as a large flow. NOTE When the bandwidth utilization of traffic that has been identified as a large flow falls below the Threshold value for the duration of the Observation Time, the traffic is no longer identified as a large flow.
Threshold (Mbps) field	The bandwidth utilization threshold (in Mbps) used to identify a flow as a large flow. If the bandwidth utilization of a flow exceeds the value throughout the Observation Time, the flow is marked as a large flow.

Action Settings

Action settings are a set of configurable parameters that determine the mitigation action taken on large flows.

Field/Component	Description
Action list	The action automatically applied to flows that have been identified as large flows. Select from the following options: • None • Drop • Redirect • Meter • Mirror • RTBH Selecting an action displays additional parameters that must be configured. You can select up to three actions, for example, if you want to create an end-to-end open flow path to redirect the traffic to third party analyzers. If you select None or RTBH (Remote Trigger Black Hole), you cannot select any other actions.

Field/Component	Description
	If you select RTBH, you can specify only L3 large flow detection settings. Any L2 or L4 settings are automatically cleared.
Action tables	Configuration information about the selected actions is displayed at the bottom of the dialog box. You can edit or delete the action by clicking the **pencil** or the **trash can** icons, respectively.

Events Page

The Brocade Flow Optimizer provides real-time information for traffic monitoring events and audit events, which can be viewed in the Events page. The real-time events shown on the page have occurred over the last few days or more.

> NOTE
> The Events pane of the Dashboard provides the same real-time events information, but only for the last 30 minutes.

Events are listed in the table on the Events page, which is refreshed every 15 seconds. You can scroll through the list to view more events. If you scroll to the bottom of the table and want to view more events, click the pagination button to go to the next page.

For each event, the following information is provided in the columns of the Events page table:

- **Severity** The icon at the left of the table indicates the severity of the event.

⊗	Critical event
⚠	Warning event
ⓘ	Information event (system-wide events that occur during the processing of flows and application of mitigation actions)

- **Time** The time the event occurred (the client time stamp).
- **Description** A brief description of the event.
- **Message ID** The unique identifier for the message.

The Events page also provides counters for real-time events.

All	The total number of events that have been logged during the last 30 of the current session.
Action	The total number of events related to monitoring traffic for large flows. These events include the setup of profiles, flows, the detection of large flows, the execution of mitigation actions and more.
Audit	The total number of events performed by users (Administrator or Operator) that have been logged during the last 30 minutes of the current session. This includes the changing of controller settings, adding, editing, or deleting profiles, and user management events.

Settings Page

The Settings page contains the tabs you use to configure the general settings (SDN Controller), manage users, and manage devices. You also use these tabs to view the current SDN Controller settings, list of system users, and the current system device settings.

General Tab

The General tab shows the current SDN Controller settings (the URL and username for the Controller) and the current email notification settings. You use the tab to view these settings and to open the dialogs you use to configure the SDN Controller settings and the email notification settings.

You configure the SDN Controller settings and the email notification settings as part of the initial application configuration (email notification settings are optional).

SDN Controller Settings dialog

Use the **SDN Controller Settings** dialog to set up the connection to the SDN Controller as part of the initial system configuration, and to edit the settings if the SDN Controller parameters change.

If the settings are incorrect, the Brocade Flow Optimizer cannot connect to the Controller.

The SDN Controller Settings dialog contains the following information:

Item	Description
IP Address	IP address of the SDN Controller.
HTTPS	Indicates whether you want secure (HTTPS) communication with the Controller. • Select the check box for secure communication over HTTPS. • Clear the check box for communication over HTTP. If you select HTTPS, make sure that HTTPS is also turned on at the Controller. By default, HTTPS is turned off.
Port	REST API port number of the Controller. Values are as follows: • 8443 for HTTPS connection (**HTTPS** check box is selected). • 8181 for HTTP connection.
Username	Username for the SDN Controller.
Password	Password for the SDN Controller.

Email Settings Dialog

You use the Email Settings dialog to set up the Brocade Flow Optimizer so that system users receive automated email notifications about events that affect traffic monitoring. You enable email notifications for the first time as part of the initial system configuration.

For detailed steps on using this dialog, see:

- Configuring email notifications on page 21

Users tab

The Users tab shows the list of current system users, including the user role (Administrator or Operator) for each user. You use the tab to view the list of current users and to open the dialogs you use to manage users.

> NOTE
> The types of user management actions you can perform varies depending on whether you have Administrator privileges or Operator privileges.

This table lists the user management actions that can be performed based on system privileges:

Privileges	User Management Actions
Admin	Add new users Edit users (change passwords)

Privileges	User Management Actions
	Delete users Change their password or the passwords of users with Operator privileges
Operator	Change their own password (cannot change passwords of other users)

Add New User Dialog

The Add New User dialog is used to add new users to the system. You must have Administrator privileges to add new users.

> NOTE
> By default, all new users added by the Administrator have Operator privileges. Users with Operator privileges cannot modify the system configuration, add new users, or delete users, create or edit profiles, or change the passwords of other users.

Complete these steps to add a new user.

1. Go to the Dashboard page.
2. Click the **Settings** tab.

   The list of current users appears.
3. Click the **+ Add new user** link (above the list of users).

   The Add New User dialog appears.
4. Type the name (username) and password for the new user in the text boxes.
5. Click **OK**.

   The new user is added to the list of current users.

Edit User Dialog

Use the Edit User dialog to change user passwords. Your system user role

> NOTE
> If you are a user with Operator privileges, you can only change your password. If you are a user with Administrator privileges, you can change your password or the password of other users.

The application also enables Administrators to delete users and add new users.

Devices tab

The **Devices** tab of the **Settings** page shows the current configuration of the system devices including the SNMP settings used for the communications between the Brocade Flow Optimizer and system devices. Use this tab to view the current device settings and SNMP communications settings.

When you select the **Devices** tab, the data is automatically refreshed to show the most current information.

The **Devices** tab is divided into the following sections:

- sFlow Collector Settings
- SNMP Settings
- Devices

sFlow Collector Settings section

This section of the **Devices** tab shows the current sFlow Controller settings. These settings are the In-band IP address and the Out-of-band IP address of the ports on the Brocade Flow Optimizer that receives sFlow samples from the device.

You configure these settings as part of the initial system configuration process. Click the **pencil** icon to change the addresses.

SNMP Settings section

This section of the **Devices** tab shows the current SNMP profiles that have been configured. The system uses these profiles during the sFlow registration process to configure sFlow destination IP address.

You define the SNMP profiles as part of the initial system configuration process.

- Click **+Add** to add additional SNMP profiles.
- Click the **pencil** icon to edit an existing profile.
- Click the **trash can** icon to delete a profile.

Devices section

This section of the **Devices** tab shows the devices that are currently registered to forward sFlow samples (registered devices) and the devices that are available to be registered to forward sFlow samples.

The **Registered** table and **Available** table in the **Devices** section show the current system devices.

- **Registered**

  This table lists all of the devices that have been registered to forward sFlow samples. You register devices as part of the initial system configuration process.

  Select the **For Trigger** check box to set the device as a trigger device for RTBH.

  You can delete devices from this list so that they are no longer a registered device and cannot forward sFlow samples.

- **Available**

  This table lists all of the devices that are available for registration, including devices that are already registered. The devices in this list have been discovered by the Controller.

  Click **Register** to register a device. If the **Register** button is grayed out, it means the device is already registered.

  The Brocade Flow Optimizer application automatically updates the **Available** table to show all of the devices (and all OpenFlow enabled ports on the devices) that have been discovered on the Controller.

  The OpenFlow ports are shown in OpenFlow port (physical port) format.

  You cannot delete devices from this list. Devices are automatically deleted from this list when they are no longer discovered by the SDN Controller. This can happen if OpenFlow is disabled on a device.

It is important that you maintain these lists to ensure they are current. Maintaining the lists is one of the key device management tasks.

sFlow Collector Settings Dialog

You use the sFlow Collector Settings dialog to set up the sFlow Collector settings as part of the initial system configuration and to edit the settings if the sFlow Collector parameters change. These settings must be configured before the Brocade Flow Optimizer server can receive sFlow samples. You configure the settings for the first time as part of the initial system configuration.

Configuring the sFlow Collector settings involves selecting the In-band and Out-of-band IP addresses for the two ports on the Brocade Flow Optimizer server that receive sFlow samples.

For detailed steps on using this dialog, see:

- Configuring the sFlow Collector settings on page 18
- Modifying or re-entering the SDN Controller settings on page 27

SNMP Settings Dialog

You use the SNMP Settings dialog to set up the SNMP communications between the Brocade Flow Optimizer server and system devices, which is essential for sFlow registration. You also use the dialog to edit existing settings if the requirements for SNMP communications change. You configure the settings for the first time as part of the initial system configuration.

Configuring SNMP settings involves defining one or more SNMP profiles, which are used by the system during the sFlow registration process. You select the version of SNMP for each SNMP profile using a drop-down menu in the dialog. The default for the SNMP version is v1/v2 (supports version 1 and 2 of SNMP).

For detailed steps on using this dialog, see:

- Configuring SNMP communication settings on page 19
- Editing v1/v2 SNMP Profiles on page 28
- Editing v3 SNMP Profiles on page 28

Register Dialog

You use the Register dialog to complete a few different device management tasks. It is used to register devices to forward sFlow samples to the Brocade Flow Optimizer server, and to change the set of ports on a device that are enabled to forward sFlow samples.

For detailed steps on using this dialog, see:

- Registering devices on page 30
- Unregistering devices on page 31
- Managing Registered Devices on page 31

Trigger Settings dialog

Use the **Trigger Settings** dialog to provide SSH login credentials for the trigger device.

The following table describes the fields in the **Trigger Settings** dialog.

Item	Description
Login Credentials: • SSH_User Name • SSH_Password	User mode credentials for logging into the trigger device with read privileges.
Configuration Credentials: • Enable User Name • Enable Password	Configuration mode credentials for logging in to the trigger device with edit privileges.

Troubleshooting

If PostgreSQL Installed on Ubuntu

Use this procedure to troubleshoot issues you may encounter with the Brocade Flow Optimizer application database. This procedure applies to systems in which PostgreSQL is running on Ubuntu.

Complete these troubleshooting steps:

1. Kill the PostgreSQL database service using port 5432 using these commands:

   ```
   lsof -t -i :5432
   ```

   ```
   kill -9 <pid>
   ```

2. Uninstall the existing Ubuntu PostgreSQL database using this command:

   ```
   >> sudo apt-get remove --purge postgresql-9.x (where x can be either 1 or 3)
   ```

3. Restart the machine (mandatory).
4. Run this command in terminal for giving soft link:

   ```
   ln -s /tmp/.s.PGSQL.5432 /var/run/postgresql/.s.PGSQL.5432
   ```

   NOTE
   If you receive the following error message, retry the command.

   ```
   ln: failed to create symbolic link '/var/run/postgresql/.s.PGSQL.5432': File exists
   remove the PostgreSQL folder under /var/run and recreate the folder.
   >> rm -rf /var/run/postgresql
   >> mkdir /var/run/postgresql
   ```

If dbinitialization is triggered with permission denied error

Use this procedure to troubleshoot issues you may encounter with the Brocade Flow Optimizer application database. This procedure applies to all system configurations.

Complete these troubleshooting steps:

1. Make sure the permissions assigned to the folder where the Brocade Flow Optimizer software is installed is set to executable.
2. If you need to change the permissions, use this command:

   >> chmod 777 /<flowoptimizer_installation folder>/.

Gathering information before contacting Support

When you need to contact Support to report an issue, you need to complete a few tasks to ensure that you have all of the information needed to report the issue.

The tasks are as follows:

- (Optional) Changing the Logging Level on page 78
- Generating Support Save Data on page 79
- Collecting Information to Report an Issue to Support on page 79

Changing the Logging Level

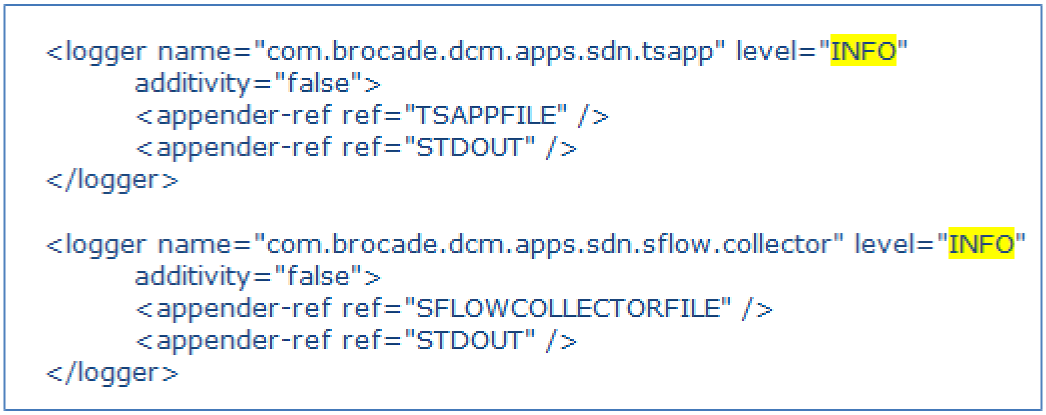
When you report an issue to Support, you can enable the logging of debug messages by changing the logging level from INFO (logging of information) to DEBUG (debugging).

> NOTE
> This task is **optional**. You do not have to change the logging level to report an issue to Support.

Pre-requisites: Make sure you have generated support save data.

Complete these steps to change the logging level to enable debugging:

1. Go to the home directory for the application (where the application files were installed).
2. Open the configuration folder.
3. Open the *logback.xml* file in any text editor.
4. Enable debugging by changing the highlighted text in this example from INFO to DEBUG.



```
<logger name="com.brocade.dcm.apps.sdn.tsapp" level="INFO"
       additivity="false">
       <appender-ref ref="TSAPPFILE" />
       <appender-ref ref="STDOUT" />
</logger>

<logger name="com.brocade.dcm.apps.sdn.sflow.collector" level="INFO"
       additivity="false">
       <appender-ref ref="SFLOWCOLLECTORFILE" />
       <appender-ref ref="STDOUT" />
</logger>
```

5. Save the changes.
6. Restart the server.

Next: Collecting information to report an issue.

Generating Support Save Data

When you report an issue to Support, you should provide details about the issue. You can easily generate details about the issue by running the support save script (*supportsave*). This information that is generated by running the script is referred to as support save data.

The data that is generated when you run the script includes:

- Database backup (includes all tables in the database)
- Configuration logs
- Application logs.

Running the script automatically triggers the database backup process and then collects the backup data along with configuration logs and application logs.

> NOTE
> You have the option of selecting the target directory where the support save data is saved. If you do not select a target directory, the backup file is automatically saved to the **SDN_HOME/support** directory (this is the default target directory).

Pre-requisites: Make sure that the database server is running. If the database server is not running, the complete database folder will be copied to the support save target directory.

Complete these steps to generate support save data.

1. Go to the directory where the Brocade Flow Optimizer application was installed.
2. Open the bin folder.
3. (Optional) Use the **sh supportsave --help** command to open the Help so you can find the syntax to use the script:
4. (Optional) Using the **target-directory** parameter of the *supportsave* script, specify the directory where you want the support save data saved. The directory name must not contain spaces. If you do not specify a directory, the default directory is automatically used (**SDN_HOME/support**).
5. Run the support save script (*supportsave*).
   The support save data is automatically saved to the target directory you specified, or to the default directory if you did not specify a directory. The data is contained in a single .tar file with this naming convention (*<flowoptimizer_home_directory>\data \supportsave\logs_<timestamp>.tar*).

Next:

- Collecting Information to Report an Issue to Support

Collecting Information to Report an Issue to Support

When you report an issue to Support, you need to collect certain information before you submit the report. Use this procedure to collect the information.

Pre-requisites: Make sure you have completed these tasks:

- (Optional) Changing the Logging Level on page 78
- Generating Support Save Data on page 79

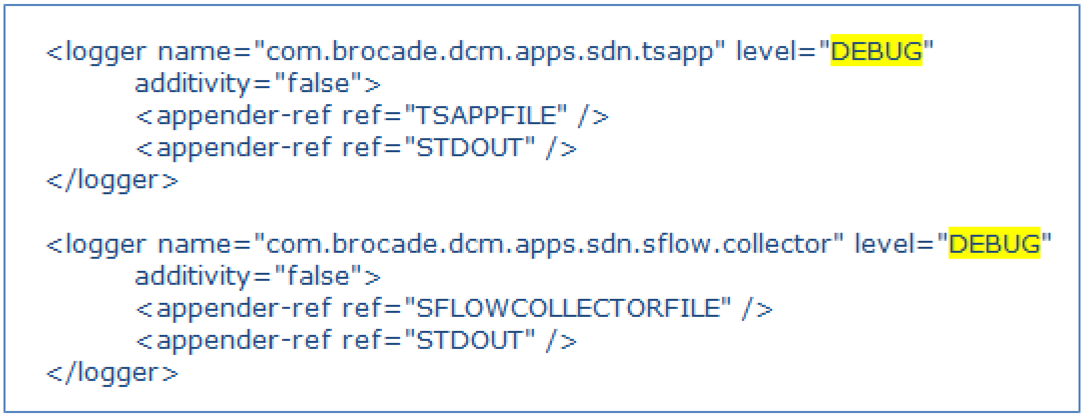
Complete these steps to collect the information:

1. Reproduce the issue.
2. Go to the directory where the support save data is stored (*<flowoptimizer_home_directory>\data\supportsave\/*).
3. Make a copy the support save file (.tar) you generated in the previous task, and email it to Support.

NOTE

If you changed the logging level from INFO to DEBUG in a previous task, you must complete the remaining steps of this procedure. If you did not change the logging level from INFO to DEBUG, you have completed the tasks required to collect the information needed to report an issue to support.

4. Open the configuration folder (it is in the home directory).
5. Open the *logback.xml* file in any text editor.
6. Change the highlighted text (as shown in this example) from DEBUG to INFO.



```
<logger name="com.brocade.dcm.apps.sdn.tsapp" level="DEBUG"
        additivity="false">
        <appender-ref ref="TSAPPFILE" />
        <appender-ref ref="STDOUT" />
</logger>

<logger name="com.brocade.dcm.apps.sdn.sflow.collector" level="DEBUG"
        additivity="false">
        <appender-ref ref="SFLOWCOLLECTORFILE" />
        <appender-ref ref="STDOUT" />
</logger>
```

7. Save the changes.
8. Restart the application.

Debugging Support

The Brocade Flow Optimizer provides a set of log files you can use for debugging purposes. The log files are installed automatically when you install the application software.

All of the log files are stored in the Logs folder in the home directory (the directory where the application files were installed). The following log files are provided:

Log File	Use
sflowcollector.log	Used to record (log) sFlow data collection data.
tsapp.log	Used to record (log) mitigation action data (on the Controller).
console.log	Used to record (log) OSGi (Open Services Gateway initiative) container data.
dbinit.log	Used to record (log) database initialization data.
sflowcollector.log	Used to record (log) database service data.

Error codes

The Brocade Flow Optimizer provides you with error messages for many of the issues you may encounter. You can use the information in the messages for troubleshooting purposes.

The types of error codes are as follows:

- Common

- Application
- sFlow Collector
- Profile validation
- sFlow settings
- Email
- User-defined flows

NOTE

Adjacent error codes may have numbers that are two or more whole numbers apart. This does not mean that an error code is missing. All of the current error codes are included.

Common error codes and messages

The following tables list the common error codes and messages.

1000	
Message	Internal server error
Message Type	AUDIT | LOG
Class	GENERAL
Severity	ERROR
Probable Cause	Indicates Brocade Flow Optimizer has encountered an error that could not be handled.
Recommended Action	If this error is impacting the functionality, and restart of the server did not resolve the error, please collect the support save and contact Brocade support.

1001	
Message	Database Exception
Message Type	AUDIT | LOG
Class	GENERAL
Severity	ERROR
Probable Cause	Indicates Brocade Flow optimizer has failed to perform the intended database operation.
Recommended Action	Verify if the database server is started properly. Verify if the host where Brocade Flow Optimizer is running has enough disk space. Please restart the application to recover. If this does not resolve the issue, please collect the support save and contact Brocade support.

1002	
Message	Exception while getting Event Profile Information from database
Message Type	AUDIT | LOG
Class	PROFILE MANAGEMENT
Severity	ERROR
Probable Cause	Indicates Brocade Flow optimizer has failed to retrieve the profiles related events from database.
Recommended Action	Verify if the database server is started properly. Verify if the host where Brocade Flow Optimizer is running has enough disk space. Please restart the application to recover. If this does not resolve the issue, please collect the support save and contact Brocade support.

1003	
Message	Exception while creating Event in database
Message Type	AUDIT | LOG
Class	EVENT MANAGEMENT
Severity	ERROR
Probable Cause	Indicates an error occurred while creating an event in the database.
Recommended Action	Verify if the database server is started properly. Verify if the host where Brocade Flow Optimizer is running has enough disk space. Please restart the application to recover. If this does not resolve the issue, please collect the support save and contact Brocade support.

1005	
Message	Exception while getting Profiles from database
Message Type	AUDIT | LOG
Class	PROFILE MANAGEMENT
Severity	ERROR
Probable Cause	Indicates Brocade Flow optimizer has failed to retrieve the profiles information from database.
Recommended Action	Verify if the database server is started properly. Verify if the host where Brocade Flow Optimizer is running has enough disk space. Please restart the application to recover. If this does not resolve the issue please collect the support save and contact Brocade support Save

1008	
Message	Device SNMP communication failed
Message Type	AUDIT | LOG
Class	SETTINGS
Severity	ERROR
Probable Cause	Indicates the SNMP communication with device is failed.
Recommended Action	Verify the SNMP communication is enabled on the device. Ensure the SNMP profile created in the Brocade Flow Optimizer has proper credentials. Ensure the SNMP port 161 is open for SNMP communication.

Application error codes

The following tables list the application error codes and messages.

1003	
Message	Failed to create user defined flow: <flow name> Action: DROP / REDIRECT / METER / REMARK / MIRROR Failed to mitigate large flow: <flow name> Action: DROP / REDIRECT / METER / REMARK / MIRROR
Message Type	AUDIT | LOG
Class	Flow Management
Severity	ERROR
Probable Cause	Indicates the application has failed to mitigate / the identified large flow on the device. This error could also indicate that the application has failed to create a user created custom flow on the device.
Recommended Action	Ensure the SDN Controller configured is reachable. If the SDN Controller is reachable, login to the device and verify the logs for identifying the reason for flow creation failure.

1008	
Message	Failed to add / update the profile. Reason: <Reason for the failure>
Message Type	AUDIT | LOG
Class	Profile Management
Severity	ERROR
Probable Cause	Indicates the application has failed to add or update the profile.
Recommended Action	The reason code mentioned in the event will have a detailed reason for the failure. This could be the validation error. Please provide the profile parameters as mentioned in the error message to resolve the issue.

1011	
Message	Failed to delete the profiles. <List of Profiles>
Message Type	AUDIT | LOG
Class	Profile Management
Severity	ERROR
Probable Cause	Indicates the application has failed to delete the selected profiles.
Recommended Action	The reason code mentioned in the event will have a detailed reason for the failure.

1013	
Message	Failed to send the email. The mail server may be down or the Server Name, User ID or Password is invalid.
Message Type	AUDIT | LOG
Class	Email
Severity	ERROR
Probable Cause	Indicates the application has failed to send the email to the configured email ID's.
Recommended Action	Please validate the email server settings and credentials. The email server might not be reachable.

sFlow Collector error codes

The following table lists the sFlow Collector error codes and messages.

Code	Message
2001	Invalid input parameters-granularity cannot be greater than duration
2002	Size of utilizations in database are not equal for populating or aggregating data
2003	Username cannot be empty. Username should not exceed 128 characters, valid characters aplhanumeric, space, -, ., _ and ~
2004	Password cannot be empty, Password length should be at least 8 characters and should not exceed 75 characters.
2005	Invalid username or password
2006	User does not exist
2007	Password encryption error - {0}
2008	User sessions have reached maximum limit
2009	Invalid token
2010	User does not have sufficient privileges
2011	Root user account cannot be deleted
2012	Duplicate user, the specified user already exists
2013	Root user account cannot be updated
2014	Invalid input parameters-start time is greater than end time

Code	Message
2015	Invalid Request, Large flow Id is null or empty
2016	Invalid Request, Profile Id is null or empty
2017	Traffic flow details is null
2018	Profile details is null
2019	Controller URL is null or empty
2020	Controller username is null or empty
2021	Controller password is null or empty
2022	Controller already exists
2023	Controller does not exist
2024	Controller url is invalid - {0}
2025	Invalid SNMP profile name, it is null or empty
2026	Invalid SNMP version
2027	Duplicate SNMP profile, the specified SNMP profile already exists
2028	Invalid auth password, it is null or empty
2029	Invalid priv password, it is null or empty
2030	SNMP profile {0} does not exist
2031	SDN Controller settings must be configured to get available devices
2032	Invalid no of SNMP profiles, two are needed for swapping
2033	Invalid device ip, ipaddress is null or empty
2034	Device {0} is already managed
2035	There are no SNMP profiles to manage device, please configure at least one SNMP profile
2036	Input port list for device {0} is empty, user has to specify at least one device port
2037	SDN Controller {0} is not reachable, please check and update SDN Controller settings
2038	Device {0} is not managed
2039	Device {0} cannot be managed because it is missing in the controller. Please delete device
2040	Cannot register on device, there are already 4 collectors on device
2041	Device {0} cannot be managed because collector is missing on device. Please delete device and add again
2042	Collector IP is missing, please configure collector
2043	Username cannot be empty
2044	Password cannot be empty
2045	The access privilege value is invalid, it can only be 0 or 1
2046	Could not find learned flow for checksum id <Checksum ID>
2047	Invalid flow id. checksum id is null or empty
2048	Invalid device ip. it is null or empty
2049	BGP is not enabled on device. <Device IP Address>
2050	CLI command failed. <Reason for Failure>
2051	There are existing RTBH static routes on the device <Device IP address>
2052	Please provide a value for the trigger query parameter
2053	Invalid ether_type. <Ethernet Type>
2054	There are no trigger devices. There should be at least one trigger device to create an RTBH flow.
2055	RTBH static route of flowID=<Flow ID> and destinationIP=<Device IP Address> and tag=<RTBH Tag> already exists on device <Device IP Address>

Code	Message
2056	Invalid device type. RTBH is only supported on NetIron

Profile validation error codes

The following table lists the profile validation error codes and messages.

Code	Message
5001	Profile Name cannot exceed more than 128 characters
5002	Invalid observation interval value. Valid observation interval (3000 ms - 3600000 ms)
5003	Invalid threshold value. Valid threshold interval (1 Mbps - 204800 Mbps)
5004	Invalid profile Type
5005	Invalid profile status
5006	Invalid user name
5007	Invalid mitigation action
5008	Priority already set. Please use different priority.
5009	Network Attributes cannot be Empty
5010	Profile cannot have same network attribute twice
5011	Destination MAC cannot be empty
5012	Source MAC cannot be empty
5013	The network attribute IN_VLAN is invalid
5014	The network attribute VLAN_PRIORITY is invalid
5015	IPv4 source address cannot be empty
5016	IPv4 destination address cannot be empty
5017	IPv6 source address cannot be empty
5018	IPv6 destination address cannot be empty
5019	IP Protocol cannot be empty
5020	DSCP cannot be empty
5021	TCP source or dest port is invalid
5022	TCP destination port cannot be empty
5023	UDP source or dest port is invalid
5024	UDP destination port cannot be empty
5025	TCP Flags cannot be empty
5026	IP fragment cannot be empty
5027	Invalid MAC Format. Please provide the MAC address in format 11:22:33:44:55:66
5028	Invalid IN VLAN String
5029	Invalid VLAN ID. Valid Range: 1 to 4095
5030	Invalid VLAN priority
5031	Invalid VLAN priority. Valid Range: 0 - 7
5032	VLAN ID has to be selected for setting VLAN priority
5033	Invalid IPv4 source address. Please enter valid IP address in CIDR format (eg: 10.5.6.7/32
5034	Invalid IPv4 destination address. Please enter valid IP address in CIDR format (eg: 10.5.6.7/32
5035	Invalid IPv6 source address. Please enter valid IP address in CIDR format (eg: 2001:0db8:0000:0000:0000:ff00:0042:8329/64

Code	Message
5036	Invalid IPv6 destination address. Please enter valid IP address in CIDR format (eg: 2001:0db8:0000:0000:0000:ff00:0042:8329/64
5037	Invalid IP Protocol. Valid values: TCP / UDP / ICMP
5038	Invalid DSCP. DSCP should be an integer value. Valid Range: 0 - 63
5039	IPv6 address cannot be selected when you want to set IPv4 source or destination
5040	IPv4 address cannot be selected when you want to set IPv6 source or destination
5041	The IP Protocol must be set to TCP when TCP Port is selected
5042	UDP Port cannot be selected when TCP port is selected
5043	The IP Protocol must be set to UDP when UDP Port is selected
5044	TCP Port cannot be selected when UCP port is selected
5045	The IP Protocol must be set to TCP when TCP Flag is selected
5046	Invalid TCP flag. Valid values: URG / ACK / PSH / RST / SYN / FIN
5047	Only yes / No is allowed for IP fragment option
5050	When redirect action selected, please provide the redirect node and port
5051	Invalid Redirect node. Valid Format Node: 10.45.67.4 Port: 1,2. Ingress and Mirror ports cannot be same
5052	The profile name\" {0} \"from query parameter and profile name \" {1} \" from profile object does not match
5053	Failed to search user name for given user ID
5054	Failed to insert profile {0}
5055	Failed to insert mitigation association {0} {1}
5056	Failed to insert profile attribute association {0} {1} {2}
5057	Failed to delete the profile {0}
5058	Failed to update profile {0}
5059	Failed to delete profile mitigation association for profile {0}
5060	Failed to delete profile attribute association for profile {0}
5061	The node with IP : {0} is not discovered in BSC
5062	Failed to create flow request. Profile Name: {0} Action: {1} Flow Key {2}
5063	Failed to Program Flow for {0} on BSC for node: {1} for destination {2}
5064	Failed to create meter for {0} on BSC for node: {1} for VLAN {2}
5065	Failed to program flow for {0} on BSC for node: {1} for VLAN {2}
5066	Failed to delete meter for {0} on BSC for node: {1} for VLAN {2}
5067	Failed to get configured nodes for programming flow: {0}
5068	Failed to create meter for {0} on BSC for node: {1}
5069	Failed to validate IP address {0} during the Large flow detection
5070	Please select NONE as an action when any of the detection only parameters are selected
5071	Ingress port is required for METER action
5072	Please provide valid Ingress node and port for METER action
5073	Only one Ingress node and port are allowed for METER / MIRROR action
5074	VLAN ID is mandatory network attribute for metering the traffic
5075	Invalid Rate limit value for meter
5076	Invalid DSCP Rate limit value for meter
5077	DSCP Remark rate limit should be less than Drop rate limit
5078	Invalid Profile Name. Only Alphanumeric, Space and - / . / _ / ~ are allowed

Code	Message
5079	Profile with name \" {0} \" already exists
5080	VLAN ID is mandatory network attribute when you select MIRROR as an action
5081	There are too many wild card attributes for the profile {0}. Maximum is 2.
5082	Action is invalid for the profile {0} with wildcard attribute. Only NONE action is supported for a profile with wildcard attribute.
5083	Maximum of 50 profiles is allowed. Please remove one or more profile(s) before adding new profile
5084	Mirror action is invalid for default profiles
5085	Ingress and Mirror port are required for MIRROR action
5086	Wildcard is not allowed on both IPv4 and IPv6
5087	Invalid Redirect node. Destination MAC address {0} is invalid
5088	Invalid Redirect node. Node IP address {0} is invalid
5089	Invalid Redirect node. Only one port is allowed when vlan ID or dest mac are specified
5090	Invalid Redirect node. Ports {0} is invalid
5091	Invalid Redirect node. Vlan ID {0} is invalid
5092	Invalid Source IP
5093	Invalid Destination IP
5094	VLAN field is mandatory for meter, mirror and remark profiles
5095	The network attribute IN_VLAN_TAGGED value is invalid
5096	The network attribute IN_VLAN is mandatory for vlan tagged profiles
5097	The property vlan_id_present is mandatory for meter, mirror, and remark flows
5098	The property vlan_id is mandatory when vlan_id_present is true
5099	The configured ingress and egress port should not be same
5100	Invalid Redirect node. For Drop action, the device IP cannot be empty
5101	Invalid vlan action. supported actions are ignore, push, pop, modify
5102	Invalid ether type value, <Ethernet Type>
5103	select atleast one action while creating the user defined flow
5104	You cannot select more than 3 actions in the user defined flow
5105	Invalid RTBH profile, <Profile Name>
5106	Ethernet Type cannot be empty
5107	Cannot select more than one action if NONE is part of the list
5108	Cannot select more than one action if RTBH is part of the list
5109	User can select only one action for default profiles
5110	Please select atleast one mitigation action while creating a custom profile
5111	Invalid DSCP Precedence value for meter. Valid Range is 0-7
5112	MAC address cannot be combined with wildcard and mask
5113	Only Destination MAC or Ingress VLAN can be removed or overwritten
5114	Please select atleast remove or overwrite values
5115	Remove and Override attributes must be mutually exclusive. <Attributes Named> is erroneously present in both
5116	We can override or remove match criteria for only Drop and Redirect actions
5117	The attribute <Attribute Name> is not selected in the original match criteria, hence it cannot be selected as a remove or override attribute
5118	The destination MAC for the overwrite MAC cannot be empty
5119	Mask of L2 destination overwrite is not supported

Code	Message
5120	The IN VLAN for the overwrite VLAN cannot be empty
5121	Only integer is allowed for VLAN overwrite
5122	Ingress port is missing while egress is present
5123	Egress port is missing while ingress is present

sFlow settings error codes

The following table lists the sFlow setting failure error codes and messages.

Code	Message
7001	Failed to retreive the sFlow settings
7002	Failed to retreive the Network interfaces from Brocade Flow Optimizer host.
7003	Failed to insert sFlow settings
7004	Failed to update sFlow settings
7005	Invalid in-band or out-of-band address

Email error codes

The following table lists the email error codes and messages.

Code	Message
8001	Failed to send mail to the recipients
8002	Invalid parameters for email configurations

User-defined flows error codes

The following table lists the user-defined flows error codes and messages.

9001	
Message	The checksum is not valid. Please provide the valid checksum
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	Indicate the invalid checksum ID is passed for the user defined flow
Recommended Action	Please provide the valid checksum ID

9002	
Message	Please provide at least one match criteria in the flow
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	Indicates user has not select any match criteria in the user defined flow
Recommended Action	Please provide at least one match criteria for the user defined flow

9003	
Message	Invalid Priority for user defined flow. Valid Priority ranges are Above Learned and Programmed: 36001-65535 and Below Learned and Programmed: 1001-32000
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	Indicates user has provided wrong Flow priority
Recommended Action	Provide valid flow priority as mentioned in the valid range

9004	
Message	Invalid IP Type. Please provide the valid type of IP Address (ipv4/ipv6) if you provide the IP address
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	Indicates user has provide invalid IP Address type
Recommended Action	Valid IP address types are IPV4 / IPV6

9005	
Message	Source Port and Destination port should be empty, if the IP Protocol is None or empty
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	Indicates user provided Layer 4 port as match criteria without selected IP Type
Recommended Action	Please select IP Type as criteria while providing the L4 port

9006	
Message	Destination port is invalid
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	
Recommended Action	

9007	
Message	Invalid redirection parameters. Ensure to set RedirectActionParameters when redirect action is selected
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	
Recommended Action	

9008	
Message	SDN Controller settings in Brocade Flow Optimizer are not configured or controller not reachable
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	Indicates user has not configured the SDN controller settings before creating the user defined flow.
Recommended Action	Please enter valid SDN controller details before creating the user defined flow

9009	
Message	No Open flow enabled ports in the device <Device IP>
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	Indicates there are no open flow enabled ports in the selected device.
Recommended Action	Please enable open flow on at least one port in the device.

9010	
Message	The device <device IP> is not discovered in controller
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	Indicates the device selected for mitigation is not discovered in the controller
Recommended Action	Please add the device to the SDN controller before configuring the mitigation action.

9011	
Message	Invalid MAC address in set destination field
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	Indicates Invalid MAC address in the modify action
Recommended Action	Provide valid MAC in 6 tuples format (ff:ff:ff:ff:ff:ff)

9012	
Message	Invalid VLAN ID in set destination field
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	Indicates invalid VLAN ID
Recommended Action	Please provide the valid VLAN ID

9013	
Message	Invalid meter parameters. Ensure to set MeterActionParameters when METER action is selected

9013	
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	Indicates the meter parameters are invalid
Recommended Action	Please provide mandatory METER parameters for the user defined flow.

9014	
Message	The port <Port Number> is not present in device <device IP>
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	Indicates the provided port number is not present in the selected device.
Recommended Action	Please provide the valid port number for the selected device.

9015	
Message	Invalid mirror parameters. Ensure to set MirrorActionParameters when MIRROR action is selected
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	
Recommended Action	

9016	
Message	The ingress port and mirror port should belong to same device.
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	
Recommended Action	

9017	
Message	The ingress port and mirror port should not be same.
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	
Recommended Action	

9018	
Message	You cannot select multiple ingress port in redirect action if you choose to set MAC or VLAN ID
Message Type	AUDIT | LOG

9018	
Class	User Defined Flows
Severity	ERROR
Probable Cause	
Recommended Action	

9019	
Message	Failed to create a user defined flow on the Device. Please verify the device logs for more information
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	Indicates Brocade Flow Optimizer has failed to create a user defined flow
Recommended Action	Please validate the device logs by commands " show log " on the device.

9020	
Message	Failed to delete a flow. Invalid Flow ID <Flow ID>
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	
Recommended Action	

9021	
Message	Invalid Priority for user defined flow. Valid Priority ranges Above Learned and Programmed: 36001 - 65535. Below Learned and Programmed: 1001 - 32000
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	
Recommended Action	

9022	
Message	The Priority <flow priority> is already used by other flow. Please provide a new priority or delete existing flow to free up the priority
Message Type	AUDIT | LOG
Class	User Defined Flows
Severity	ERROR
Probable Cause	Indicates there is already a flow with same priority.
Recommended Action	Please provide the unused priority.

9023	
Message	Hard-timeout is invalid. Only non-negative numbers are accepted
Message Type	AUDIT | LOG

9023	
Class	User Defined Flows
Severity	ERROR
Probable Cause	Indicates the Hard Timeout of the flow is invalid.
Recommended Action	Only the positive number of timeout is valid.