53-1003997-02
November 30, 2015

Brocade Flow Optimizer

User Guide

Supporting Brocade Flow Optimizer 1.1

BROCADE

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

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names Identifies keywords and operands Identifies the names of user-manipulated GUI elements Identifies text to enter at the GUI
italic text	Identifies emphasis Identifies variables Identifies document titles
`Courier font`	Identifies CLI output Identifies command syntax examples

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, **--show** WWN.

Convention	Description
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options. In Fibre Channel products, square brackets may be used instead for this purpose.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

You can download additional publications supporting your product at www.brocade.com. Select the Brocade Products tab to locate your product, then click the Brocade product name or image to open the individual product page. The user manuals are available in the resources module at the bottom of the page under the Documentation category.

To get up-to-the-minute information on Brocade products and resources, go to MyBrocade. You can register at no cost to obtain a user ID and password.

Release notes are available on MyBrocade under Product Downloads.

White papers, online demonstrations, and data sheets are available through the Brocade website.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers contact their OEM/Solutions provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to http://www.brocade.com/services-support/index.html.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone	E-mail
Preferred method of contact for non-urgent issues: • My Cases through MyBrocade • Software downloads and licensing tools • Knowledge Base	Required for Sev 1-Critical and Sev 2-High issues: • Continental US: 1-800-752-8061 • Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33) • For areas unable to access toll free number: +1-408-333-6061 • Toll-free numbers are available in many countries.	support@brocade.com Please include: • Problem summary • Serial number • Installation details • Environment description

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/Solution Provider, contact your OEM/Solution Provider for all of your product support needs.

- OEM/Solution Providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/Solution Provider.

- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/Solution Provider.

Document feedback

To send feedback and report errors in the documentation you can use the feedback form posted with the document or you can e-mail the documentation team.

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com.
- By sending your feedback to documentation@brocade.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Getting Started

Before you can begin using the Brocade Flow Optimizer application, you need to complete some preliminary tasks, including installing the application software and the initial configuration.

You should also become familiar with some basic tasks that you will perform on a regular basis.

- System Requirements on page 10
- Initial System Configuration on page 14
- Common User Tasks on page 27

Introduction to Brocade Flow Optimizer

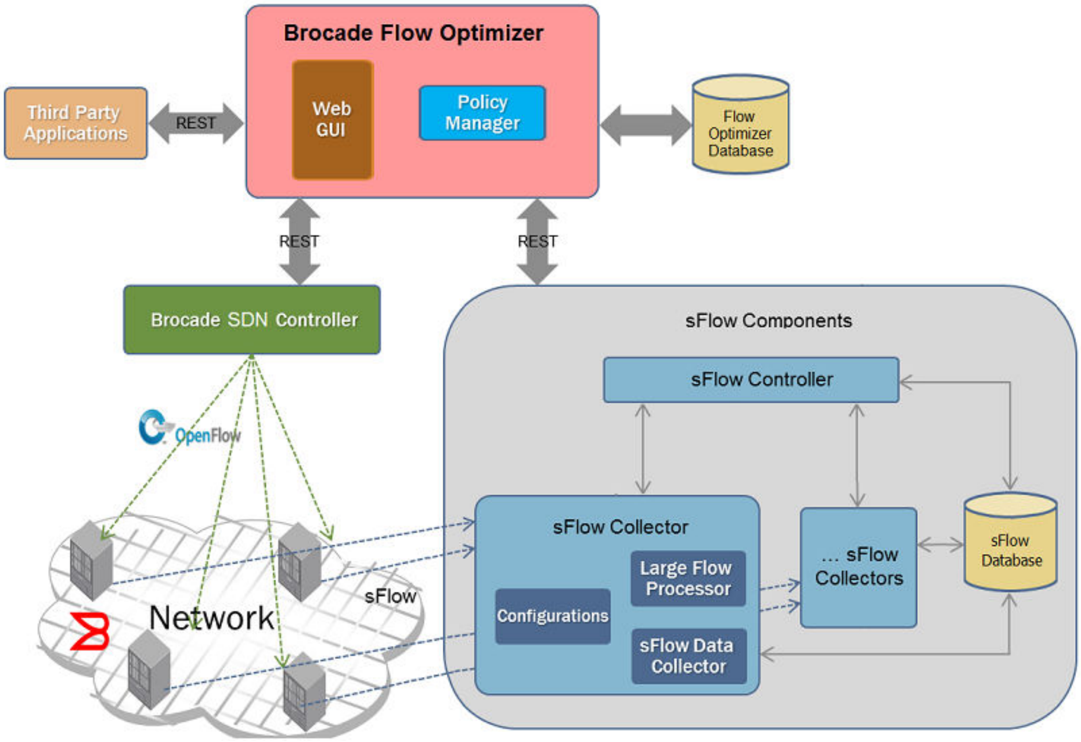
The Brocade Flow Optimizer application is designed to enable you to optimize the traffic flows on your network by providing you with the ability to monitor and control flows that exceed the bandwidth utilization you have established for the flows.

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.



System Requirements

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

NOTE
Be sure to follow the instructions provided with any software you need to download and install.

Hardware

The following table lists the hardware required to use the Brocade Flow Optimizer.

Host Server	
	Operating System Linux (one of the following): - Ubuntu 14.0.4 (64 Bit) - CentOS 7 (64 Bit)
	Memory 16GB RAM
	ConnectivityServer needs to have In-band connectivity to receive sFlow packets from MLX devices.

	Hard Disk Drive 256GB of free HDD space
	Core Processors A minimum of 4 core processors.
Brocade Devices	
	One or more of the following: • **FastIron** ICX 6610, ICX 7450, or ICX 7750. • **NetIron** MLXe

Software

The following table lists the software required to use the Brocade Flow Optimizer.

MLX NetIron firmware, version NI 5.9a. Download the NetIron firmware from http://my.brocade.com.
ICX FastIron firmware. The firmware requirements vary depending on the device. • ICX 6610 (requires FastIron 08.0.30a) • ICX 7450 or ICX 7750 (requires FastIron 08.0.40)
OpenFlow, version 1.3.

Browser

The following table lists the browser required to use the Brocade Flow Optimizer.

Google Chrome

OpenFlow Controller

The following table lists the OpenFlow Controller required to use the Brocade Flow Optimizer.

One of the following:	
Brocade SDN Controller (version 2.1.0)	Download the SDN Controller from http://my.brocade.com.
OpenDayLight (ODL)	Lithium SR2

Limitations

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

All ICX devices

The known limitations for this release are:

- **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 6610

The known limitations for this release are:

- **FastIron firmware support** This device does not support FastIron 08.0.40.
- **Mirror mitigation action** This device does not support the use of the Mirror mitigation action, due to a hardware limitation.
- **Redirect mitigation action** Profile with the Redirect action cannot have **Ingress VLAN ID** as a VLAN matching field, due to a limitation on the device that causes the original VLAN tag (in incoming packets) to be dropped.

ICX 7450 and ICX 7750

The known limitations for this release are:

- **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:

- 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:

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

Installing the Software

The steps you use to install the Brocade Flow Optimizer software are the same, regardless of your operating system. The application software is a single archive distributable (.tar), which you need to download and install on your host server.

Pre-requisites: Make sure that:

- All of the required software is installed (see System Requirements on page 10 for the required software).

Complete these steps to install the Brocade Flow Optimizer software.

1. Download the Brocade Flow Optimizer application software (*Flowoptimizer_<version>_rc_<build#> -distribution.tar*).
2. Enter the following command to extract the .tar installation file (*tar –xvf flow_optimizer_<version>-distribution.tar*) to the directory where you want the application files to be installed. This will be the home directory for the application.

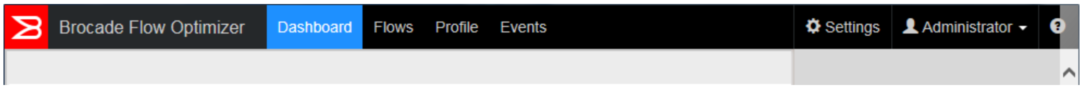
NOTE
Complete the remaining steps to verify that the application was installed successfully. These steps show you how start the application and log in.

3. Go to the home directory for the application.
4. Go to bin folder.
5. 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**
6. Log in to the application by opening your browser, then point the browser 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.
7. Select or click the option to continue with the connection.
   The Login page appears.
8. Log in.
   The Dashboard page appears.



Next steps: Complete the initial system configuration. You must complete this task before you can use the Brocade Flow Optimizer application.

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
  - **(OpenDayLight)** Enabling Host Tracker No Flood Hybrid Mode on the ODL Controller
- Enabling OpenFlow on the MLX router
- Enabling OpenFlow on ICX devices
- Setting up the connection to the SDN Controller
- Configuring the sFlow Collector settings
- Configuring the SNMP communication settings
- (Optional) Setting up email notifications

Enabling the BSC Controller's Host Tracker No Flood Hybrid Mode

Before you can successfully register devices with, or reconnect devices to the Brocade SDN (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 that:

- All of the required software is installed (see System Requirements on page 10 for the required software).
- You have installed the Brocade Flow Optimizer application software (see the *Brocade Flow Optimizer User Guide* for the installation procedure).
- You have access to the latest version of the *Brocade SDN Controller User Guide*. You use it complete steps **1**, **2**, and **4** 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 (see the *Brocade SDN Controller User Guide* for details).
2. Stop the controller (see 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 (see the *Brocade SDN Controller User Guide* for details).

Enabling the ODL Controller's Host Tracker No Flood Hybrid Mode

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 that:

- All of the required software is installed (see System Requirements on page 10 for the required software).
- You have installed the Brocade Flow Optimizer application software (see the *Brocade Flow Optimizer User Guide* for the installation procedure).
- You have access to the latest version of the *Open Day Light SR2 User Guide*. You use it complete steps **1**, **2**, and **4** 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 (see the *Open Day Light SR2 User Guide* for details):
   - odl-restconf
   - odl-l2switch-hosttracker
2. Stop the controller (see 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 (see the *Open Day Light SR2 User Guide* for details).

Enabling OpenFlow on MLX Router

Before you can begin using the 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 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 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 desired interfaces.

   ```
   NetIron MLX-4 Router(config)#interface ethernet 1/1

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

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

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

   - 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 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.

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

- 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 (system reload is required once you change the system maximum values). The system maximum values are:

   - 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

NOTE
For a standalone ICX 6610, the maximum number of flows allowed is 3000.

```
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.

Pre-requisites: Make sure that you have already enabled OpenFlow on your system devices (including ICX and MLX devices).

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 times you need to enter the IP address of the Controller is when you change the configuration of your Controller and the IP address of the Controller has changed.

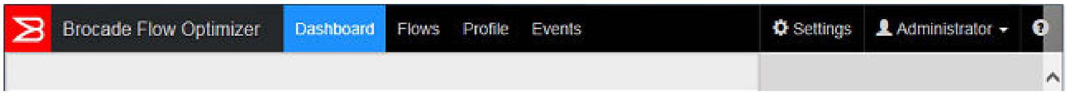
Complete these steps to start the Brocade Flow Optimizer application, log in, and complete the initial configuration of the Controller settings.

1. Go to the home directory for the application software distributable archive.
2. Go to 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 by opening your browser, then point the browser to the following URL:

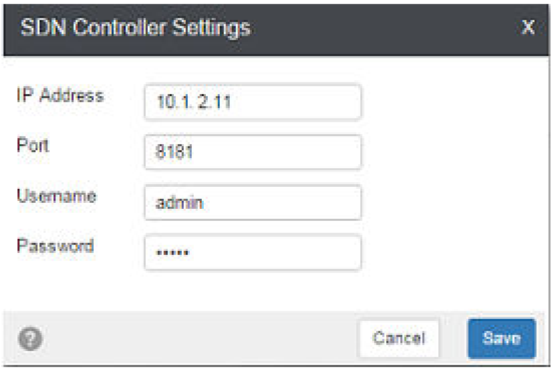
   https://<IP address of server>:8089

   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.
5. Select or click the option to continue with the connection.
   The Login page appears.
6. Log in.
   The Dashboard page appears.



7. Click the **Settings** tab.
   The General tab appears.
8. Do the following:
   a) Click the **Add+** button.
      The SDN Controller Settings dialog appears.
   b) In the **IP Address** box, type the IP address of the Controller.
   c) In the **Port** box, type the REST API port number of the Controller, which is **8181**.
   d) In the **Username** box, type the username for the OpenFlow Controller.
   e) In the **Password** box, type the password for the OpenFlow Controller.


SDN Controller Settings

IP Address: 10.1.2.11
Port: 8181
Username: admin
Password: •••••

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 appears that the Controller is unreachable. This can be caused by:

- 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 or ICX 6610 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. Enter the following command to enable sFlow null0-sampling on the MLX device.
   ```
   MLX-4 router(config)# sflow null0-sampling
   ```
2. Enter the following command to enable sampling of dropped packets on the ICX 6610 device.
   ```
   ICX6610-48 router(config)# sflow sample-mode all
   ```

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 that:

- You have completed setting up the connection to the SDN Controller.
- You have enabled sFlow sampling of dropped packets for MLX and ICX6610 devices. (For ICX7750 and ICX7450, it is enabled by default.)
- You know the correct In-band address and Out-of-band address IP 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.

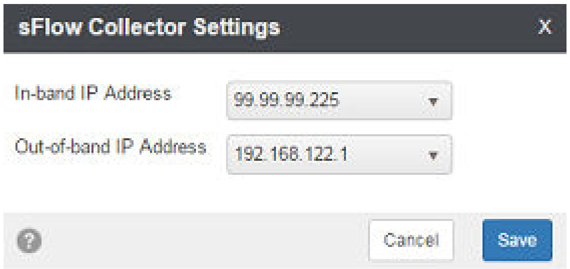
Configuring the sFlow Collector settings involves selecting the sFlow destination IP addresses for the devices. One IP address is named the In-band address, the other is named the Out-of-band address. You select the IP address based on the device type (ICX or MLXe).

- 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. Go to the **Settings** page.
2. Click the **Devices** tab.
3. Click **+Add** next to sFlow Collector Settings.
   The sFlow Collector Settings dialog appears.



sFlow Collector Settings

In-band IP Address: 99.99.99.225

Out-of-band IP Address: 192.168.122.1

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.

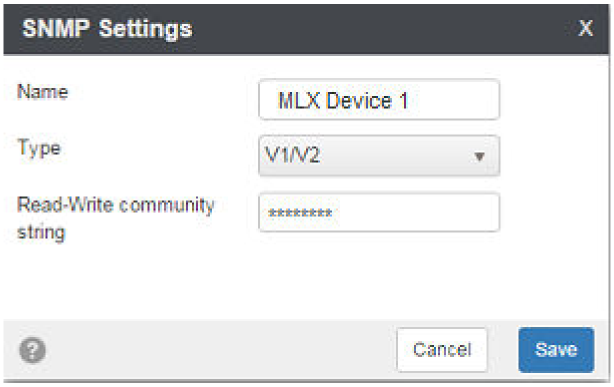
Pre-requisites: Before you begin the procedure, make sure that:

- 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.



Name: MLX Device 1

Type: V1/V2

Read-Write community string: ********

4. Do the following:
   a) In the **Name** box, type a name for the profile. (For example, the network name or device name.)
   b) Using the **Type** menu, 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 steps 1 through 5 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.

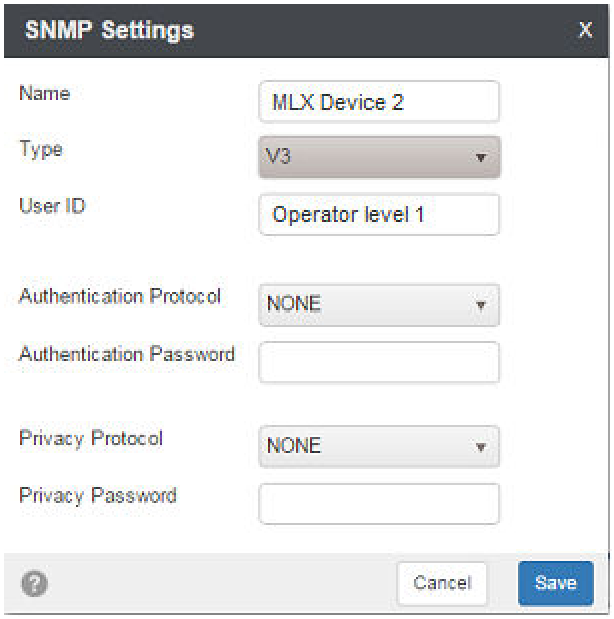
Pre-requisites: Before you begin the procedure, make sure that:

- 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.



SNMP Settings

Name: MLX Device 2

Type: V3

User ID: Operator level 1

Authentication Protocol: NONE

Authentication Password:

Privacy Protocol: NONE

Privacy Password:

4. Do the following:
   a) In the **Name** box, type a name for the profile. (For example, the network name or device name.)
   b) Using the **Type** menu, select **V3**.
   c) In the **User ID** box, type the User ID for the profile. (For example, the name of the group of users.)
   d) Using the **Authentication Protocol** menu, select the protocol to be used to encrypt the SNMP messages.
   e) In the **Authentication Password** box, type the authentication password. The correct password is required to enable the encryption of the SNMP messages.
   f) Using the **Privacy Protocol** menu, 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** box, 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. (Optional) Repeat steps 1 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.

Setting up Email Notifications

The Brocade Flow Optimizer can be set up so that system users receive automated email notifications about events that affect traffic monitoring. This helps you to ensure that system users do not have to constantly monitor the system to be aware of important events that affect traffic monitoring. You must have Administrator privileges to set up email notifications.

By default, the feature is not configured or enabled. You must configure the email notification options and enable the feature. You determine which users receive notifications about traffic monitoring events when you configure the email notification options. You can enable or disable the notifications at any time, and you can edit the settings at any time.

Email Notification Event Types

All users that you 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:

- 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 1 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). **NOTE** 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.

TABLE 1 Flow-related Events (Continued)

Event	Description	Message
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 2 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). **NOTE** 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).

TABLE 2 Profile-related Events (Continued)

Event	Description	Message
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).

Setting up or Editing Email Notifications

You can easily set up the Brocade Flow Optimizer so that system users receive automated email notifications about events that affect traffic monitoring. You must have Administrator privileges to set up or edit email notification settings.

NOTE
You use the same procedure to set up or edit the email notification settings.

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

- You have the SMTP port number and SMTP identifier (ID) for the email server (the server that sends the notifications to the specified set of system users).
- That you have the reply address. This is the email ID (address) that sends the notifications to the specified set of system users.
- Each user you want to set up to receive email notifications has a valid email account. You need their email address to complete the procedure.

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

1. 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 checkbox.
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.

Common User Tasks

There are some common tasks that you perform on a regular basis as part of day-to-day operations. These tasks can be easily completed using just a few steps.

These basic tasks include:

- Starting the Application on page 27
- Stopping the Application on page 28
- Logging In on page 28
- Logging Out on page 29
- Checking the Application Version on page 29

Starting the Application

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

Pre-requisites: The application must be installed on the host server, and you must have access to the server. Other than having access to the host server, there are no pre-requisites for starting the application. The following table lists the login pre-requisites by user type:

User Type	Pre-requisites
Administrator	User account (You do not have to create one. When the application is installed on the host server, a default user with the username Administrator is created.)
Operator	User account must be created by Administrator.

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. Use one of the following commands to run the **startservice** script (this starts the application):
   - **(Root user) sh startservice**, or
   - **(Root user) ./startservice**

- **(Non-root user) sudo sh startservice**, or
- **(Non-root user) sudo ./startservice**

Stopping the Application

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

Complete these steps to stop the application.

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
   - **(Root user) ./stopservice**
   - **(Non-root user) sudo sh stopservice**, or
   - **(Non-root user) sudo ./stopservice**

   A message appears indicating that the application was stopped successfully.

Logging In

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

Pre-requisites: You cannot login if the application is not running (started). If you want to login, make sure the application is started.

NOTE
When the Brocade Flow Optimizer software is installed, an Administrator user is automatically created. If you are an Administrator and are logging in for the first time, use the following credentials:

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

Complete these steps to login.

1. Open your browser and point it to the following URL:
   https://<IP address of server>:8089/

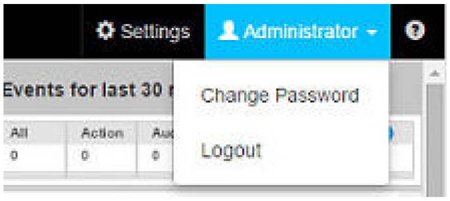
   NOTE
   The port number must be 8089.

   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 boxes.
4. Press **Enter** or click the **blue arrow**.
   The Dashboard page of the application appears.

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.

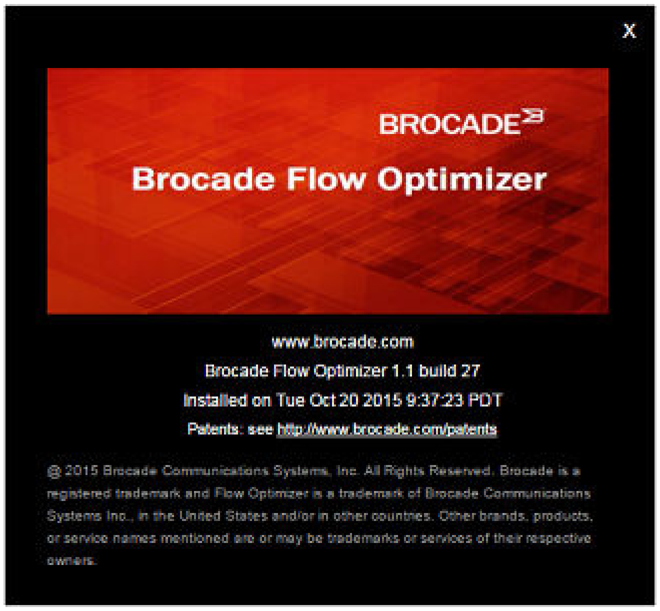
3. (Optional) Close your browser.

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.



BROCADE

Brocade Flow Optimizer

www.brocade.com

Brocade Flow Optimizer 1.1 build 27

Installed on Tue Oct 20 2015 9:37:23 PDT

Patents: see http://www.brocade.com/patents

@ 2015 Brocade Communications Systems, Inc. All Rights Reserved. Brocade is a registered trademark and Flow Optimizer is a trademark of Brocade Communications Systems Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or services of their respective owners.

Backing up the Database

You can easily backup 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.

NOTE
You have the option of specifying the backup type (full or partial) and the target directory for the backup (these are optional selections). If you do not make selections for these items, or if the values you specify are invalid, the default backup type and target directory are automatically used.

The default backup type and target directory are:

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

Complete these steps to backup 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) Choose the backup type you want using the **backup-type** parameter of the *dbbackup* script. The possible values are:
    - **Partial**: Some tables are excluded from the backup.
    - **Full**: All database tables are included in the backup (this is the default).
5. (Optional) Using the **target-directory** parameter of the *dbbackup* 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/backup/databases**).
6. Use the following command to run the back 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 easily 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 procedure below for restoring the database provides the steps required to restart the database.

Complete these steps to backup the database:

1. Extract the distribution to one location (a single folder).
2. Run the *installdatabase* script (this 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. Use the following command to run the restore script (*dbrestore*).

   - **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 support save 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. Run the *startservice* script to start the application.

Device Management

After you complete the initial configuration process, you can easily manage the system devices using the Devices tab of the Settings page. Managing devices is an essential administrator task that ensures all of the system devices you need to use to enforce your traffic policy are available for use.

The Brocade Flow Optimizer application provides all of the functionality required to ensure that you can configure the connections between devices and other system components, as well as set up devices so they are able to receive sFlow samples for traffic monitoring purposes.

The different types of tasks involved in device management include:

- Modifying or re-entering the sFlow Collector settings.
- Registering devices (enables devices to forward sFlow samples).
- Unregister devices (disables devices so they cannot forward sFlow samples).
- Modifying the current sFlow registration for a device.
- Modifying the sFlow sampling rate for a device.
- Deleting a device so it is no longer available for registration.

Available devices and registered devices

The Devices tab contains two lists that are used to show the status of all system devices on which OpenFlow has been enabled. The two lists are **Available** devices and **Registered** devices.

Available devices	The devices in this list represent devices on which OpenFlow has been enabled, and: • Is being actively monitored or managed by the SDN Controller. • Is **not** enabled to forward sFlow samples.

Registered devices

The devices in this list represent all of the devices that can be used to forward sFlow samples to the Brocade Flow Optimizer application for analysis.

A device that is listed as **registered** is a device on which:

- OpenFlow has been enabled.
- The Brocade Flow Optimizer application has been registered on the device, which enables the device to forward sFlow samples. This process is referred to as registering devices.

When you register a device, you configure one or more ports on the device as destination ports for sFlow samples.

You can unregister a device so that it is no longer able to forward sFlow samples. When you unregister a device, the device is automatically:

- Removed from the Registered list
- Added to the Available list.

NOTE
All devices listed in the Manage section of the Devices tab are currently enabled to forward sFlow samples.

Modifying or Re-entering the SDN Controller Settings

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

Pre-requisites: Make sure that:

- Start the Brocade Flow Optimizer application.

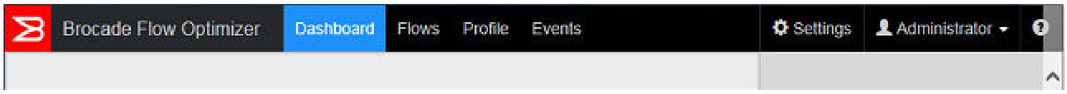
Complete these steps to modify or re-enter the Controller settings.

1. Log in to the application by opening your browser, then point the browser to the following URL:

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

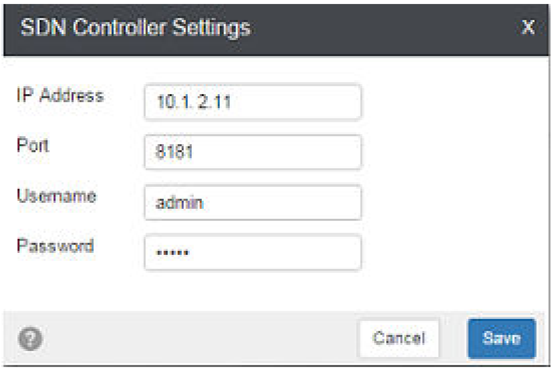
   The port number **must** be 8089. (This is the port number for the Brocade Flow Optimizer application.)

   A page appears with an alert that the connection may not be secure.
2. Select or click the option to continue with the connection.
   The Login page appears.
3. Log in.
   The Dashboard page appears.



4. Click the **Settings** tab.
   The General tab appears.
5. Click the **Edit** button next to Controller Settings.
   The SDN Controller Settings dialog appears.
6. Modify or re-enter the following SDN Controller Settings as needed:

a) **IP Address:** Type the IP address of the Controller.
b) **Port:** Type the REST API port number of the Controller, which is **8181**.
c) **Username:** Type the username for the OpenFlow Controller.
d) **Password:** Type the password for the OpenFlow Controller



SDN Controller Settings

IP Address: 10.1.2.11
Port: 8181
Username: admin
Password: •••••

7. 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 appears that the Controller is unreachable. This can be caused by:

- 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.

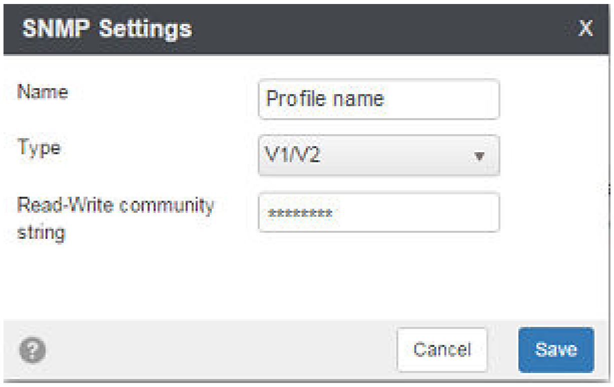
Editing v1/v2 SNMP Profiles

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.



SNMP Settings

Name: Profile name

Type: V1/V2

Read-Write community string: ********

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.

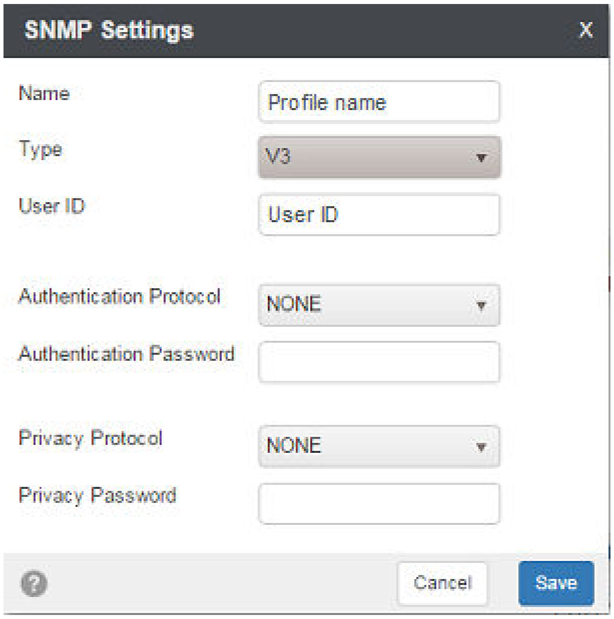
Editing v3 SNMP Profiles

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.



Name: Profile name
Type: V3
User ID: User ID
Authentication Protocol: NONE
Authentication Password:
Privacy Protocol: NONE
Privacy Password:

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.

About Registering and Unregistering Devices

Registering and unregistering devices are tasks you use to manage devices after you complete the initial system configuration.

NOTE
Before you can register a device, you must enable OpenFlow on the device, which is one of the initial system configuration tasks.

Registering devices

When you register a device, you are actually registering the Brocade Flow Optimizer application on the device as the destination for sFlows. This enables the device to forward sFlow samples to the Brocade Flow Optimizer application. A second part of device registration is to select the ports on the device that you want to receive the sFlow samples.

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.

Unregistering devices

A device that is currently registered can be unregistered. Unregistering a device disables the device from forwarding sFlow samples. The device cannot be used to forward sFlow sample until it is registered again. When you unregister a device, it is removed from the Manage list and is added to the Available list of the Devices tab.

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.

Column	Description
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). You 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.
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 is a device management task that must be completed so that devices can receive flows from the SDN Controller and forward sFlows to the Brocade Flow Optimizer application.

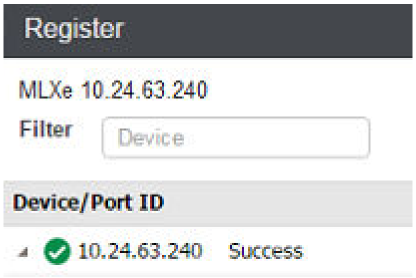
Pre-requisites: Before you can register a device, you must complete the initial system configuration to ensure that OpenFlow has been enabled on the device. You cannot register a device unless OpenFlow has been enabled on the device.

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. You use the Devices tab of the Settings page to register a device.

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. 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, click the **checkbox** for the device or devices you want to register.
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.



Register

MLXe 10.24.63.240

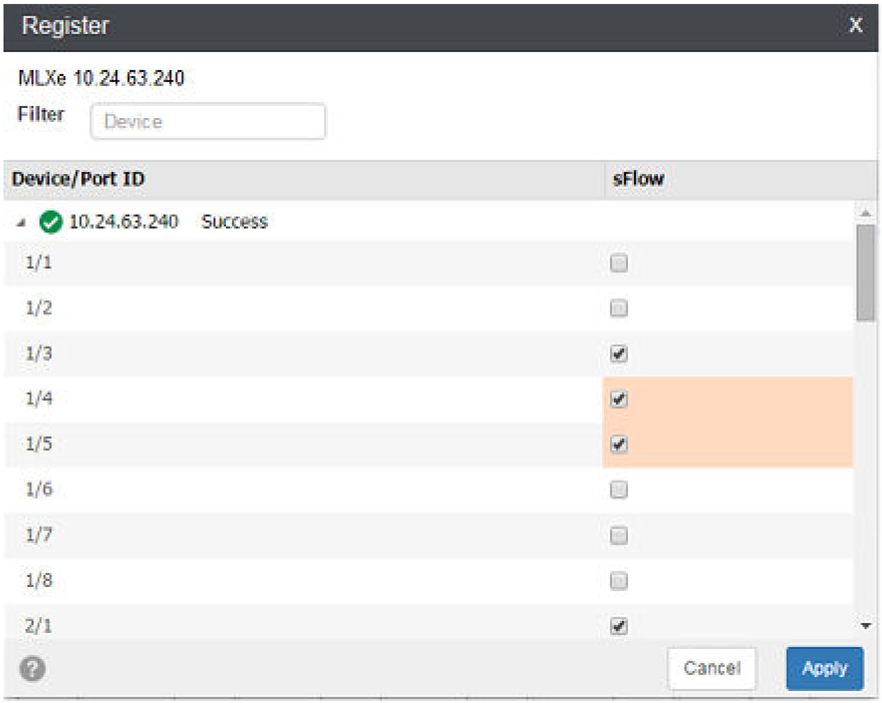
Filter: Device

Device/Port ID	
✓ 10.24.63.240	Success

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.

   The following figure shows the Register dialog. In this example, ports 1/3, 1/4, 1/5, and 2/1 have been selected as sFlow forwarding ports.



MLXe 10.24.63.240

Filter: Device

Device/Port ID	sFlow
10.24.63.240 Success	
1/1	☐
1/2	☐
1/3	☑
1/4	☑
1/5	☑
1/6	☐
1/7	☐
1/8	☐
2/1	☑

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

Unregistering Devices

Unregistering devices is a device management task that you use to disable sFlow forwarding on a device. Once the device is unregistered, it cannot forward sFlow samples to the Brocade Flow Optimizer server.

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.

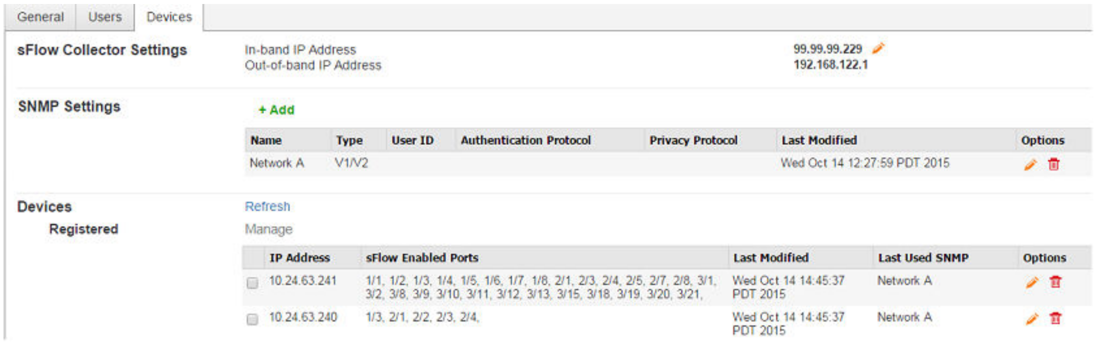
1. Select the **Settings** page.
2. Click the **Devices** tab.
   The Registered list in the tab shows all devices that are currently registered.
3. In the Registered list, click the **checkbox** for the device or devices you want to unregister.
4. Click the **Delete** link (in the Options column) for 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.

The following figure shows the Devices tab. In this example, there are two devices currently registered (shown in the Registered list). The Manage option is disabled because no devices have been selected (you select a device by checking the checkbox at the left side of the table).



sFlow Collector Settings

In-band IP Address 99.99.99.229
Out-of-band IP Address 192.168.122.1

SNMP Settings

Name	Type	User ID	Authentication Protocol	Privacy Protocol	Last Modified	Options
Network A	V1/V2				Wed Oct 14 12:27:59 PDT 2015	

Devices

Registered

	IP Address	sFlow Enabled Ports	Last Modified	Last Used SNMP	Options
□	10.24.63.241	1/1, 1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 2/1, 2/3, 2/4, 2/5, 2/7, 2/8, 3/1, 3/2, 3/8, 3/9, 3/10, 3/11, 3/12, 3/13, 3/15, 3/18, 3/19, 3/20, 3/21,	Wed Oct 14 14:45:37 PDT 2015	Network A	
□	10.24.63.240	1/3, 2/1, 2/2, 2/3, 2/4,	Wed Oct 14 14:45:37 PDT 2015	Network A	

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.

Deleting a Device so it is Not Available for Registration

One of the device management tasks is to make sure that the list of devices that are available for registration includes only the devices that you need to be available for registration. This makes it easier to find devices in the list when you need to register the device.

The Available table in the Devices tab of the Settings page lists all of the devices that are currently available to be registered (only registered devices can receive sFlow samples). 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.

Complete these steps to delete a device so it is no longer available for registration.

1. 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, click the **checkbox** for the device you want to delete.
4. Click the **Delete** link (in the Options column) for the devices you selected.
5. Repeat steps **3** and **4** to delete additional devices from the Available list.
6. Click the **Refresh** button to refresh the lists of Devices (the button is above the Register table).
   The Available list is updated to reflect your changes. The devices you deleted are no longer in the list of Available devices.

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 application's configuration properties file (*config.properties*). Because devices must be re-registered before the changes to the sampling rate takes effect, you must do the following after you edit the *config.properties* file.

- Restart the Brocade Flow Optimizer server.
- Unregister all devices that are currently registered.
- Re-register all devices.

1. Go to Brocade Flow Optimizer home directory (the directory where the application was installed. the configuration properties file (*config.properties*) .
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

The Brocade Flow Optimizer application enables you to manage system users to ensure you can create and maintain user accounts as needed.

The different types of user management tasks include:

- Adding New Users on page 45
- Editing Users on page 46
- Editing Users on page 46

Adding New Users

You add new users as part of your user management tasks. You must have Administrator privileges to add new users.

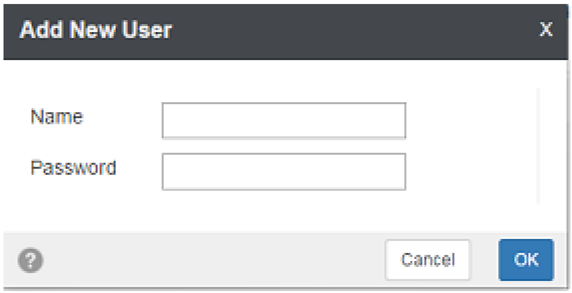
The process for adding a new user involves specifying the name (username) and password for the user. Once the new user is added, they can use the Brocade Flow Optimizer application to:

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

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.

Use this procedure 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.

Editing Users

The Brocade Flow Optimizer enables you to edit users as part of your user management and system security tasks. Editing users involves changing user passwords.

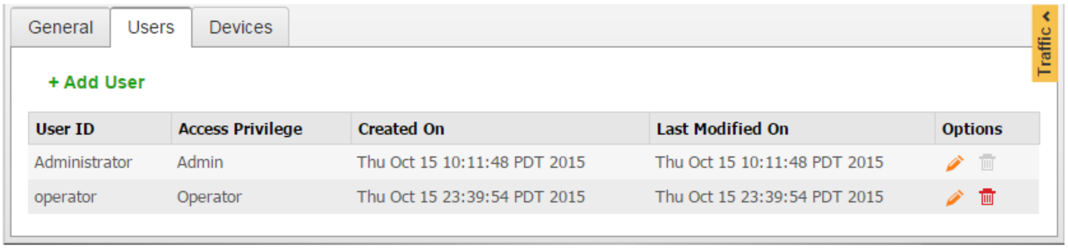
All users can change their own password. Only a user with Administrator privileges can change the passwords of other users.

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. Based on your user role (Administrator or Operator), log in as follows:
   - (Administrator) Login as the user you want to edit.
   - (Operator) Login using your current credentials.
2. Go to the **Settings** page, and click the **Users** tab.

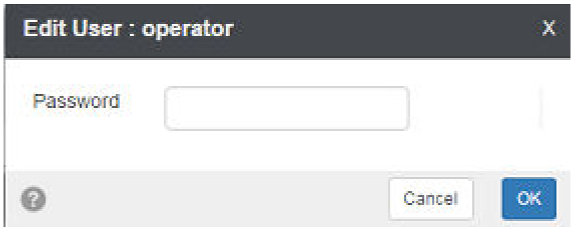
   The tab shows the list of current users.



User ID	Access Privilege	Created On	Last Modified On	Options
Administrator	Admin	Thu Oct 15 10:11:48 PDT 2015	Thu Oct 15 10:11:48 PDT 2015	✎ 🗑
operator	Operator	Thu Oct 15 23:39:54 PDT 2015	Thu Oct 15 23:39:54 PDT 2015	✎ 🗑

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 in the **Password** box, 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

Profiles are the main components of your traffic management policy enforcement. You manage the profiles in your traffic management policy by configuring profiles, modifying (editing) profiles, and enabling or disabling profiles.

You use the Policy page of the application to view the current profiles in your traffic management policy and to open the dialogs you use to configure, edit, and enable or disable profiles.

About Profiles

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 the desired mitigation action for any large flow that is detected. Once you configure the mitigation action in the profile, the system automatically executes the action on any large flow that is detected by the profile.

You configure profiles by setting values for profile parameters that determine:

- 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 type of mitigation action to be taken once a traffic flow is detected. The available mitigation actions vary depending on whether the profile is a default profile or a custom default profile.

Basic types of profiles

The Brocade Flow Optimizer provides two basic types of profiles you can use to monitor traffic. They are:

- Default profiles (see Default Profiles on page 49).
- Custom profiles (see Custom Profiles on page 51).

Default Profiles

There are a total of 7 Default profiles provided with the application for detecting volumetric traffic on your network. You use these profiles to detect and mitigate a variety of traffic that can consume network resources, disrupt your 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. You use the Edit Profiles dialog to edit them.

NOTE
You cannot delete default profiles, which you can do with Custom profiles.

This table lists and describes the default profiles:

DNS Reflection	This profile is used to monitor and detect unrequested DNS query responses coming from third party systems (usually name servers). The third party systems are responding to DNS queries sent from a source (or 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's network resources and disrupt the network. The mitigation actions available for this profile are Drop, Redirect, and None.
NTP Reflection	This profile is used to monitor and detect unrequested responses from NTP servers. The NTP servers are responding to get monlist requests from a source (or 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's network resources and disrupt the network. The mitigation actions available for this profile are Drop, Redirect, and None.
ICMP Ping flood	This profile is used to monitor and detect ICMP echo requests (Ping packets) that did not originate in your network. The requests are a continuous series of Ping packets from a source (or 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.
UDP flood	This profile is used to monitor and detect 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.
CharGen	This profile is used to monitor and detect 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.
Quote of the Day	This profile is used to monitor and detect 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	This profile is used to monitor and detect 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.

Custom Profiles

The Brocade Flow Optimizer provides a highly configurable type of profile (called Custom profiles) that you can use along with the Default profiles to enforce your traffic management policy.

Like Default profiles, Custom profiles are designed to enable you to detect large flows and apply mitigation actions to flows that have been detected as large 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, Meter, Remark, 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. You use the Add Profile dialog to create new custom profiles, and the Edit Profiles dialog to edit them.

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

Maximum number of 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.

Creating and Editing Profiles

The Brocade Flow Optimizer enables you to create and edit profiles to ensure you effectively enforce your traffic management policy.

Although you can edit both Default and Custom profiles, you can create only Custom profiles. Custom profiles are highly configurable: you can create variations to effectively enforce your traffic management policy.

NOTE
You must have Administrator privileges to create or edit profiles.

The following table lists the types of create and delete operations that can be performed based on the profile type:

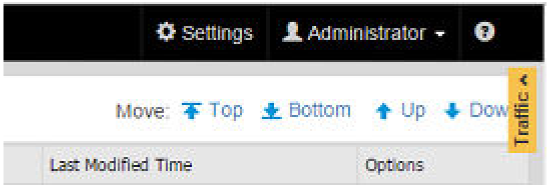
Type	Create	Edit
Custom	Yes You can create Custom profiles as needed to enforce your traffic management policy. **NOTE** The Brocade Flow Optimizer supports up to 50 Custom profiles.	Yes You can modify all of the settings of a Custom profile (including the profile name).

Type	Create	Edit
Default	No	Yes You can modify the mitigation action of Default profiles. You cannot modify the large flow detection settings or the profile name.

Changing the profile priority

Changing the priority of profiles enables you to manage the order in which profiles are validated when monitoring traffic. Profiles are validated starting with the profile at the top of the list, which is the profile with highest priority. Moving profiles down the list decreases the priority: moving profiles up the list increases the priority.

You can change the priority of profiles directly from the Profile page by moving profiles up and down in the list using the Top, Bottom, Up, and Down buttons (you use them to move multiple profiles at the same time).



Deleting custom profiles

You can delete Custom profiles as part of your profile management tasks. Deleting Custom profiles enables you to remove profiles that you no longer use to enforce your traffic management policy. You can delete Custom profiles directly from the Profile page.

NOTE
You cannot delete Default profiles.

Large Flow Detection Parameters

The large flow detection parameters are configurable parameters that determine which traffic layer or layers are inspected during traffic monitoring. This enables you to define custom profiles you can use to effectively enforce your traffic management policy.

You must configure these parameters when you create new custom profiles. If you need to change the settings to adapt to changes in your traffic management policy, you can edit these settings. The large flow detection settings are grouped based the network layer that corresponds to the options available in each group. The groups are layer 2 (L2), layer 3 (L3), and layer 4 (L4).

You do not configure the large flow detection settings for default profiles. These settings are pre-defined in the default profiles that are provided with the Brocade Flow Optimizer software and cannot be changed.

NOTE
You have the option of using wildcards as matching criteria for many of the large flow detection parameters. See Using Wildcards as Matching Criteria in Custom Profiles on page 57for more information.

To ensure that the settings you enter are accepted and take effect, make sure that you enter all of the values correctly. The following table lists the requirements for specifying the large flow detection parameter settings, including the format requirements for using wildcards.

Layer	Attribute	Description	Input Format	Requirement
L2	SRC MAC	Source MAC address	• Standard entry: 12:73:51:22:79:99 • Wildcard: * / FF : * : GG : * : * : * / EMPTY	Valid MAC address in 6 tuples separated by : (colon).
L2	DST MAC	Destination MAC address		
L2	In VLAN (Tagged, Untagged)	Ingress Vlan ID	• Standard entry: Comma separated VLAN IDs • Wildcard: EMPTY / * / 10, 11 / 10 – 12	The Vlan IDs must be configured on the device. **NOTE** If you configure this parameter, you must also configure the L2 802.1q parameter.
L2	802.1q	Vlan Priority	• Standard entry: Value from 1 to 7 • Wildcard: EMPTY / * / 1, 2 / 1 – 5	**NOTE** If you configure this parameter, you must also configure the L2 **In VLAN** parameter.
L3	Source IP V4	IPV4 source IP address	• Standard entry: Valid IPV4 address. Can use subnet mask or arbitrary bitmask • Wildcard: EMPTY / * / 10.3.4.5/32	Combination of IPV4 and IPV6 is not allowed. You must select either IPV4 source and destination, or IPV6 source and destination.
L3	Destination IP V4	IPV4 destination IP address		
L3	Source IP V6	IPV6 source IP address	• Standard entry: Valid IPV6 address. Can use subnet mask or arbitrary bitmask. • Wildcard: EMPTY / * / 2001:cdba:9abc:5678::/64	You can use subnet mask or arbitrary bitmask in CIDR format. For example: • ipv6: 2001:cdba:9abc:5678::/64 • ipv4: 10.3.4.5 or 10.3.4.5/32
L3	Destination IP V6	IPV6 destination IP address		
L3	IP protocol	IP protocol	• Standard entry: TCP, UDP, or ICMP • Wildcard: ANY / TCP / UDP / ICMP	You must select the protocol from the list.

Layer	Attribute	Description	Input Format	Requirement
L3	DSCP	Di_ Serv Code Point (part of the IPv4). ToS field or the IPv6 Traffic Class field.	- Standard entry: Value from 0 to 63 - Wildcard: EMPTY / * / 1, 2 / 1 – 5	
L3	IP Fragment	Yes, No	- Standard entry: Yes / No - Wildcard: (Not supported)	**NOTE** This is a detection-only parameter. If you select this option, the **None** mitigation is automatically selected by the system. No mitigation action is applied.
L4	TCP SRC PORT	TCP source port	- Standard entry: Valid port number - Wildcard: EMPTY / * / 23, 53 / 21 – 51	IP protocol must be selected as TCP.
L4	TCP DST PORT	TCP destination port		
L4	UDP SRC PORT	UDP source port		IP protocol must be selected as UDP.
L4	UDP DST PORT	UDP destination port		
L4	TCP Flags	TCP Flags	- Standard entry: SYN, FIN, ACK, RST, URG, or PSH - Wildcard: (Not supported)	IP protocol should be selected as TCP. **NOTE** This is a detection-only parameter. If you select this option, the **None** mitigation is automatically selected by the system. No mitigation action is applied.

Mitigation Parameters

The mitigation parameters are configurable profile parameters that determine the conditions that must be met before traffic flows are identified as large flows and the mitigation action taken on the large flows.

Most of these parameters are common to both Default profiles and Custom profiles. You configure these parameters when:

- You create new Custom profiles.
- You edit Custom profiles or Default profiles.

The mitigation parameters are:

- Observation Time
- Threshold (Mbps)
- Action

Observation Time

The following table lists the description of this mitigation parameter and any options available for this parameter.

Description
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. **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)

The following table lists the description of this mitigation parameter and any options available for this parameter.

Description
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

Configuring this mitigation parameter determines which mitigation action is automatically applied by the system flows that have been identified as large flows. The options are:

- None (Default and Custom profiles)
- Drop (Default and Custom profiles)
- Redirect (Default and Custom profiles)
- Remark (Custom profiles only)
- Meter (Custom profiles only)
- Mirror (Custom profiles only)

NOTE
If you choose the Mirror action, make sure that you configure Mirror ACLs on the MLX using the CLI before you create mirror flows.

The following table lists the description of this mitigation parameter and any options available for this parameter.

Action mitigation parameter options

None: No mitigation action is taken. Use this 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 the device you select to receive the traffic. You use the Node Ports Picker dialog to select the device and ports. You can change the VLAN ID and destination MAC.

Meter: The traffic rate is limited (metered) to the bandwidth utilization you specify using the **Rate Limit Bandwidth** parameter. This action is only available for custom profiles based on matching vlan ids.

You have two options when using the Meter mitigation action. They are **Meter with drop band**, and **Meter with DSCP Remark band**.

NOTE
You can use **Meter with drop band** alone. If you want to use the **Meter with DSCP Remark band**, you must use it together with the **Meter with drop band** option.

- **Meter with drop band**

  The flow is metered (rate-limited) to the **Rate Limit Bandwidth** value you specify. All the traffic above the rate limit is dropped.

  If you use this Meter option, you must configure the following:

  - **Ingress Node and Port**: The node IP address and port number of the ingress (input) port of the traffic used to create the flow. Must be a single port. You use the Node Ports Picker dialog to select the device and ports.

    NOTE
    The ingress port must be part of the vlan you specify using the **Ingress VLAN ID** option.

  - **Ingress VLAN ID**: The vlan ID or IDs for creating the flow. The ingress port must be part of vlan ID you specify. To specify multiple vlans, enter the IDs in comma separated format (ID 1, ID 2, ID 3). If you specify multiple vlans, the large flows are identified separately for each vlan.
  - **Rate Limit Bandwidth**: The bandwidth utilization rate (in Mbps) used to limit the flow. The rate of the flow is limited to the value you specify.

- **Meter with DSCP Remark band**

  The DSCP remark is used to decrease the drop-precedence of the DSCP field in the IP header of the packet. When the system applies the DSCP remark, all packets that exceed the **Remark Rate** you specify are modified. The DSCP precedence value of these packets is set to the **DSCP Precedence** value you specify. You have the option of selecting a node and ports from the node received from the Controller.

  If you use this Meter option, you must configure the following:

  - **DSCP Rate limit**: The maximum bandwidth utilization for the DSCP remark.
  - **DSCP Precedence**: The value of the drop-precedence field in the IP header.
  - **Ingress Node and Port**: The node IP address and port number of the ingress (input) port of the traffic used to create the flow. Must be a single port. You use the Node Ports Picker dialog to select the device and ports.

    NOTE
    The ingress port must be part of the vlan you specify using the **Ingress VLAN ID** option.

  - **Ingress VLAN ID**: The vlan ID or IDs for creating the flow. The ingress port must be part of vlan ID you specify. To specify multiple vlans, enter the IDs in comma separated format (ID 1, ID 2, ID 3). If you specify multiple vlans, the large flows are identified separately for each vlan.

Mirror: 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, **and**
- You do not want the flow altered, or any other flows altered.

NOTE
This action is only available for Custom profiles.

The replicated flow is a duplicate or copy of the original flow being monitored (called a mirrored flow). The port that receives the mirrored flow is called the mirror port. You specify the mirror port when you configure the custom profile.

You must configure the following parameters when you select this action:

- **Ingress Port**: The port that receives the flow being monitored. You select this port from the list of nodes on the Controller. You must select a single port.

  NOTE
  If you are using a NetIron device, you must select a port that is tagged as an IN_VLAN port. This restriction does not apply to FastIron devices.
- **IN_VLAN**: (Required only for tagged VLAN matching. For untagged VLAN matching, you do not have to specify this parameter.) The IN_VLAN network attribute for the ingress port. This ensures that the ingress port is a part of the VLAN ID defined in the Custom profile.
- **Mirror Port**: The port that receives the replicated flow. You can select only one port.

  NOTE
  Make sure that you have configured Mirror ACLs on the MLX using the CLI before you create mirror flows.

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.

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.

You use the Add Profile dialog to create new Custom profiles. Once the new Custom profile is created, you can easily begin using it to monitor traffic.

When you create new Custom profiles, you must configure two basic types of settings. They are:

Large flow detection settings	Used to determine the network layer or layers that are inspected during traffic monitoring.
Mitigation settings	Used to define the conditions that must be met before a flow is identified as a large flow, and the mitigation action that is applied to large flows.

NOTE
Make sure you are familiar with the large flow detection parameters and mitigation action parameters, see Large Flow Detection Parameters on page 52 and Mitigation Parameters on page 54.

Options for including VLAN matching criteria in the profile

In addition to the large flow detection settings and the mitigation actions, you can choose to include or not include VLAN matching criteria in the profile. The basic options are:

- No VLAN matching

  No VLAN matching operation is performed. To use this option, do not select the VLAN option when you create the profile. This option supports the Drop and Redirect mitigation actions.
- Tagged VLAN

  Tagged VLAN matching is performed. To use this option, select the VLAN option (one of the network attribute options) when you create the profile. You must also specify the VLAN ID and VLAN priority. This option supports all mitigation actions (Drop, Redirect, Meter, Remark, and Mirror).
- Un-tagged VLAN

Un-tagged VLAN matching is performed. To use this option, select the VLAN option (one of the network attribute options) when you create the profile. Do not specify the VLAN ID or VLAN priority. This option supports all mitigation actions (Drop, Redirect, Meter, Remark, and Mirror).

The process for creating a new Custom profile involves:

- Naming the profile and entering a description.
- Configuring the large flow detection settings.
- Configuring the mitigation action settings.

Pre-requisites: 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).

Complete these steps to create a new Custom profile:

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

   NOTE
   The maximum length of the profile name is 128 Character. A profile name can contain only alpha numeric characters and special characters like (- / . / _ / ~).

4. In the **Description** box, type a description for the profile.

   NOTE
   Steps **5**, **6**, and **7** are for selecting the network layers for the profile (L2, L3, or L4). You can select any combination of layers, but you must select at least one layer. For each layer you select, you must specify the source and destination addresses, ports, and any other mandatory items.

5. (Optional) In the **Large flow detection settings** section, select the **L2** checkbox.
   a) Specify the **Source MAC** address for the flow.
   b) Specify the **Destination MAC** address for the flow.
   c) Specify the **Ingress Vlan ID** for the flow.
   d) Specify the **VLAN Priority** for the flow.
6. (Optional) In the **Large flow detection settings** section, select the **L3** checkbox.
   a) Specify the **Source IP (IPv4)** address for the flow.
   b) Specify the **Destination IP (IPv4)** address for the flow.
   c) Specify the **Source IP (IPv6)** for the flow.
   d) Specify the **Destination IP (IPv6)** for the flow.
   e) Specify the **IP Protocol** for the flow.
7. (Optional) In the **Large flow detection settings** section, select the **L4** checkbox.
   a) Specify the **TCP Source Port** address for the flow.
   b) Specify the **TCP Destination Port** address for the flow.
   c) Specify the **UDP Source Port** for the flow.
   d) Specify the **UDP Destination Port** for the flow.
   e) Specify the **TCP Flags** for the flow.
8. Do one of the following to select the desired VLAN matching criteria options:

- To exclude VLAN matching criteria, do not select the **VLAN** checkbox. Go directly to step **9**.
- To include tagged or untagged VLAN matching criteria, select the **VLAN** checkbox. In the dialog that appears, select the tagged or untagged option.

9. In the **Mitigation settings** section, enter the amount of time in the **Observation Time** box that you want to monitor traffic before a flow is identified as a large flow.
10. In the **Threshold (Mbps)** box, enter the bandwidth utilization threshold (in Mbps) that a flow must exceed before it is identified as a large flow.
11. Using the **Action** menu, choose one of the following mitigation actions:

- **None** No mitigation action is taken.
- **Drop** The flow is blocked.
- **Redirect** Traffic is redirected to a port or ports on the device you select to receive the traffic. (You can change the VLAN ID and Destination MAC.)
- **Meter** (Applies only to Custom profiles based on matching vlan IDs.) The traffic rate is limited (metered) to the bandwidth utilization you specify using the **Rate Limit Bandwidth** parameter. Choose either the **Meter with drop band** or the **Meter with DSCP Remark band** option.

NOTE
You can use **Meter with drop band** alone. If you want to use the **Meter with DSCP Remark band**, you must use it together with the **Meter with drop band** option.

- **Meter with drop band**: The flow is metered (rate-limited) to the **Rate Limit Bandwidth** value you specify. All the traffic above the rate limit is dropped. You must configure the following:
  - **Ingress Node and Port**: The node IP address and port number of the ingress (input) port of the traffic used to create the flow. Must be a single port.

    NOTE
    The ingress port must be part of the vlan you specify using the **Ingress VLAN ID** option.

  - **Ingress VLAN ID**: The vlan ID or IDs for creating the flow. The ingress port must be part of vlan ID you specify. To specify multiple vlans, enter the IDs in comma separated format (ID 1, ID 2, ID 3).
  - **Rate Limit Bandwidth**: The bandwidth utilization rate (in Mbps) used to limit the flow. The rate of the flow is limited to the value you specify.
- **Meter with DSCP Remark band**: The DSCP remark is used to decrease the drop-precedence of the DSCP field in the IP header of the packet. Packets that exceed the **Remark Rate** you specify are modified, and the DSCP precedence value is set to the **DSCP Precedence** value you specify. You must configure the following:
  - **DSCP Rate limit**: The maximum bandwidth utilization for the DSCP remark.
  - **DSCP Precedence**: The value of the drop-precedence field in the IP header.
  - **Ingress Node and Port**: The node IP address and port number of the ingress (input) port of the traffic used to create the flow. Must be a single port.

    NOTE
    The ingress port must be part of the vlan you specify using the **Ingress VLAN ID** option.

  - **Ingress VLAN ID**: The vlan ID or IDs for creating the flow. The ingress port must be part of vlan ID you specify. To specify multiple vlans, enter the IDs in comma separated format (ID 1, ID 2, ID 3).

- **Mirror** (Applies only to Custom profiles.) The flow being monitored is replicated and directed to a port (the mirror port) for further analysis. You must configure the following:

- **Ingress Port**: The port that receives the flow being monitored. You select this port from the list of nodes on the Controller. You must select a single port.
- **IN_VLAN**: The IN_VLAN network attribute for the ingress port. This ensures that the ingress port is a part of the VLAN ID defined in the Custom profile.
- **Mirror Port**: The port that receives the replicated flow. You can select only one port.

NOTE
The number of additional steps you must complete varies depending on the mitigation action you selected in the previous steps. If you:

- Selected either **None** or **Drop**, you do not need to complete any additional steps. Click **OK** to save the profile.
- If you selected **Redirect**, **Meter** or **Mirror**, you must complete steps **12**, **13**, **14**, and **15**. You use these steps to select the device and port or ports for the traffic.

12. Click the blue **Add** button to open the Node Ports Picker (you use it to select the node and ports for the profile).

    The Node Ports Picker dialog appears.
13. In the **Nodes** text box, type the IP address of the device you want to receive the redirected, metered, or mirrored traffic.
    The IP address you specified is listed under the Node heading in the dialog, and the ports of the device are listed under the IP address of the node.
14. In the list of ports, check the box next to the port or ports you want to receive the redirected, metered, or mirrored traffic.

    NOTE
    If you selected **Meter** for the mitigation action, you must select only a single port. If you selected **Redirect** for the mitigation action, you can select multiple ports.

    The port or ports you selected are listed under the Egress or Ingress heading in the dialog. (The heading is Egress if the mitigation action is **Redirect**, and it is Ingress if the mitigation action is **Meter** or **Mirror**.)
15. In the **Node Ports Picker** dialog, click **OK**.
    The node and port (or ports) are selected for the profile.
16. In the **Add Profile** dialog, click **OK**.
    The profile is created and appears in the list of profiles on the Policy page.

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 profiles and Custom profiles.

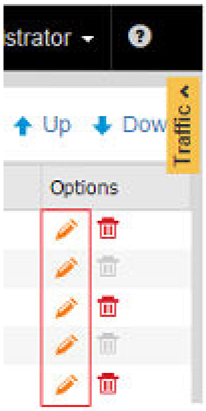
The types of changes you can make to a profile varies depending on the profile type (Default or Custom). The major task when editing profiles involves modifying the values of profile parameters.

The following table lists the types of modifications that are possible when you edit profiles.

Profile Type	Configurable Settings	Steps
Custom	Large Flow Detection Settings	See Changing Large Flow Detection Parameter Settings on page 63
	Mitigation Settings	See Changing Mitigation Parameter Settings on page 64

Profile Type	Configurable Settings	Steps
Default	Mitigation Settings	See Changing Mitigation Parameter Settings on page 64

You use the Edit Profile dialog to edit profiles. You can open this dialog directly from the Profile page by clicking the **pencil icon** in the Options column for the profile.



Changing Large Flow Detection Parameter Settings

You can modify the large flow detection parameter settings of custom profiles. This enables you to change the profiles as needed to adapt to changes in your network traffic management policy. These settings determine which traffic layer or layers that are inspected during traffic monitoring.

You use the Edit Custom Profile dialog to change the large flow detection settings of custom profiles. The detailed steps you use to change these settings are the same as the steps used to define these settings when you create custom profiles.

NOTE
Make sure you are familiar with the requirements for configuring the network layer settings (for example, MAC addresses need to be entered in a specific format). See Large Flow Detection Parameters on page 52 for details.

Complete these steps to change the large flow detection settings of a custom profile:

1. Go to the application Dashboard.
2. Make sure the Policy page is selected.
3. In the **Profile Name** column, find the name of the custom profile you want to edit.
4. In the Options column for the profile, click **Edit**.
   The Edit Custom Profile dialog appears.

   NOTE
   Steps **5**, **6**, and **7** are for selecting the network layers for the profile (L2, L3, or L4). You can select any combination of layers, but you must select at least one layer. For each layer you select, you must specify the source and destination addresses, ports, and any other mandatory items.
5. (Optional) In the **Large flow traffic detection settings** section, select the **L2** checkbox.

a) Specify the **Source MAC** address for the flow.
b) Specify the **Destination MAC** address for the flow.
c) Specify the **Ingress Vlan ID** for the flow.
d) Specify the **VLAN Priority** for the flow.

6. (Optional) In the **Large flow traffic detection settings** section, select the **L3** checkbox.

   a) Specify the **Source IP (IPv4)** address for the flow.
   b) Specify the **Destination IP (IPv4)** address for the flow.
   c) Specify the **Source IP (IPv6)** for the flow.
   d) Specify the **Destination IP (IPv6)** for the flow.
   e) Specify the **IP Protocol** for the flow.

7. (Optional) In the **Large flow traffic detection settings** section, select the **L4** checkbox.

   a) Specify the **TCP Source Port** address for the flow.
   b) Specify the **TCP Destination Port** address for the flow.
   c) Specify the **UDP Source Port** for the flow.
   d) Specify the **UDP Destination Port** for the flow.
   e) Specify the **TCP Flags** for the flow.

8. Click **OK** to save the changes.

(Optional) If you want to change the mitigation settings of the profile, see Changing Mitigation Parameter Settings on page 64.

Changing Mitigation Parameter Settings

You can modify the mitigation parameter settings of profiles. This enables you to change profiles as needed to adapt to changes in your network traffic management policy. These settings determine the conditions that must be met before a flow is detected as a large flow, and the mitigation action taken once a flow is detected as a large flow.

You can use this procedure to modify the mitigation settings of custom profiles or default profiles.

NOTE
For detailed descriptions of the mitigation parameters, see Mitigation Parameters on page 54.

Use this procedure to modify the mitigation settings.

1. Go to the application Dashboard.
2. Make sure the Profile page is selected.
3. In the **Profile Name** column, find the name of the profile you want to edit.
4. In the Options column for the profile, click **Edit**.
   If you are editing a default profile, the Edit Profile dialog appears. If you are editing a custom profile, the Edit Custom Profile dialog appears.
5. In the **Mitigation settings** section, enter the amount of time in the **Observation time** box that you want to monitor traffic before a flow is identified as a large flow.
6. In the **Threshold (Mbps)** box, enter the bandwidth utilization threshold (in Mbps) that a flow must exceed before it is identified as a large flow.

   The next step is used to modify the settings for the **Action** parameter. If you want to modify the Meter mitigation action settings, make sure you are familiar with the options for this parameter (see Mitigation Parameters on page 54).

7. Using the **Action** menu, choose one of the following mitigation actions:

   - **None** No mitigation action is taken.
   - **Drop** The flow is blocked.

- **Redirect** Traffic is redirected to a port or ports on the device you select to receive the traffic.

NOTE
The next action (Meter) applies only to custom profiles based on matching vlan ids.

- **Meter** The traffic rate is limited (metered) to the bandwidth utilization you specify using the **Rate Limit Bandwidth** parameter. Choose either the **Meter with drop band** or the **Meter with DSCP Remark band** option.

NOTE
You can use **Meter with drop band** alone. If you want to use the **Meter with DSCP Remark band**, you must use it together with the **Meter with drop band** option.

  - **Meter with drop band**: The flow is metered (rate-limited) to the **Rate Limit Bandwidth** value you specify. All the traffic above the rate limit is dropped. You must configure the following:
    - **Ingress Node and Port**: The node IP address and port number of the ingress (input) port of the traffic used to create the flow. Must be a single port.

      NOTE
      The ingress port must be part of the vlan you specify using the **Ingress VLAN ID** option.
    - **Ingress VLAN ID**: The vlan ID or IDs for creating the flow. The ingress port must be part of vlan ID you specify. To specify multiple vlans, enter the IDs in comma separated format (ID 1, ID 2, ID 3).
    - **Rate Limit Bandwidth**: The bandwidth utilization rate (in Mbps) used to limit the flow. The rate of the flow is limited to the value you specify.
  - **Meter with DSCP Remark band**: The DSCP remark is used to decrease the drop-precedence of the DSCP field in the IP header of the packet. Packets that exceed the **Remark Rate** you specify are modified, and the DSCP precedence value is set to the **DSCP Precedence** value you specify. You must configure the following:
    - **DSCP Rate limit**: The maximum bandwidth utilization for the DSCP remark.
    - **DSCP Precedence**: The value of the drop-precedence field in the IP header.
    - **Ingress Node and Port**: The node IP address and port number of the ingress (input) port of the traffic used to create the flow. Must be a single port.

      NOTE
      The ingress port must be part of the vlan you specify using the **Ingress VLAN ID** option.
    - **Ingress VLAN ID**: The vlan ID or IDs for creating the flow. The ingress port must be part of vlan ID you specify. To specify multiple vlans, enter the IDs in comma separated format (ID 1, ID 2, ID 3).

NOTE
If the selected mitigation action is either **Redirect** or **Meter**, you must complete the remaining steps if you want to change the device and ports for the redirected or metered traffic. If the selected mitigation action is either **None** or **Drop**, click **OK** to save the changes to the profile (you do not need to complete any additional steps).

8. Click the blue **Add** button to open the Node Ports Picker (you use it to select the node and ports for the profile).

   The Node Ports Picker dialog appears.
9. In the **Nodes** text box, type the IP address of the device you want to receive the redirected or metered traffic.

The IP address you specified is listed under the Node heading in the dialog, and the ports of the device are listed under the IP address of the node.

10. In the list of ports, check the box next to the port or ports you want to receive the redirected or metered traffic.

NOTE
If you selected **Meter** for the mitigation action, you must select only a single port. If you selected **Redirect** for the mitigation action, you can select multiple ports.

The port or ports you selected are listed under the Egress or Ingress heading in the dialog. (The heading is Egress if the mitigation action is **Redirect**, and it is Ingress if the mitigation action is **Meter**.)

11. In the **Node Ports Picker** dialog, click **OK**.
The node and port (or ports) are selected for the profile.

12. In the **Edit Profile** dialog, click **OK**. (If you are editing a custom profile, the dialog is the **Edit Custom Profile** dialog.)
The changes you made to the profile are saved.

Changing the Priority of a Profile

A priority is automatically assigned by the system 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.

Profile priority determines the order in which the system validates currently defined profiles when sFlow samples are received. The current priority ranking of the profiles you have configured is reflected in the list of profiles in the Profile page. Profiles higher in the list (at or near the top of the list) have a higher priority than profiles that are further down in the list. Profiles are validated in the order they appear in the list on the Profile page.

NOTE
When the system 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.

To change the priority of profiles

You have two basic options for changing the priority of a profile. You can make granular changes to the priority of a profile by moving it up or down in the list one row at a time. You can also change the priority of a profile to the highest or lowest possible priority by moving the profile to the top of the list (highest priority), or to the bottom of the list (lowest priority).

Granular changes	
To **increase** the priority	Click the **Move Up** button until the profile has the desired priority.
To **decrease** the priority	Click the **Move Down** button until the profile has the desired priority.
Change to the highest or lowest possible priority	
To change to the **highest** possible priority	Click the **Top** button.
To change to the **lowest** possible priority	Click the **Bottom** button.

Enabling and Disabling Profiles

You must enable one or more profiles before you 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.

You can easily enable or disable profiles directly from the Profile page. You have two basic options for enabling or disabling profiles. You can enable or disable individual profiles (one profile at a time), or you can enable or disable multiple profiles at the same time. Profiles that have a green checkmark are currently enabled: profiles with a red checkmark are currently disabled.

NOTE
The system automatically ignores invalid selections. For example, if you accidentally select profiles that are already enabled before clicking the **Enable** option, the system enables all profiles you selected that are disabled, and ignores invalid selections.

To enable or disable one or more profiles, do the following:

1. Make sure the Profile page is selected.
2. Click the **checkbox** next to each profile you want to enable or disable.
3. Do one of the following:
    - Click the **Enable** option above the table. All the profiles you selected are now enabled.
    - Click the **Disable** option above the table. All the profiles you selected are now disabled.

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

The Brocade Flow Optimizer application provides a browser-based graphical user interface (GUI) client that both system administrators and system users use to perform all of the tasks that are essential for their roles. The GUI utilizes REST API's exposed by the application.

The GUI provides access the application Dashboard, which you use to view information about traffic flows currently being monitored using profiles. It also contains pages used for system configuration, managing system users and traffic monitoring profiles, and for viewing traffic and real-time events.

You use the various GUI pages and dialogs to:

- Login and logout.
- Configure and manage the system, including:
  - Configuring settings required to communicate with the Controller.
  - Managing system devices.
  - Creating traffic flows to be monitored using profiles.
  - Managing profiles used to monitor traffic.
  - Managing system users.
- View traffic being monitored by the system, including:
  - Viewing a snapshot of current traffic bandwidth (all traffic currently blocked and being allowed to pass through the system).
  - Viewing the traffic flows that are currently exceeding the specified bandwidth threshold (called large traffic flows).
  - Viewing details about traffic flows currently being monitored.
- View information about traffic monitoring profiles, including:
  - Viewing all active traffic monitoring profiles.
  - Viewing details about traffic monitoring profiles (for example, bandwidth threshold or other parameter settings).
- View real-time events, including:
  - Viewing important traffic monitoring events (for example, a flow is identified as a large flow, or a flow was created or deleted).
  - Viewing system management (operational) events.
- View information about traffic flows, including:
  - View a list of all flows that are currently large flows (flows that have exceeded bandwidth threshold).
  - View a list of all flows that are being monitored but are not currently defined as large flows (not above the specified bandwidth threshold).
  - View a list of flows that have been created but are not currently being monitored.

Login Page

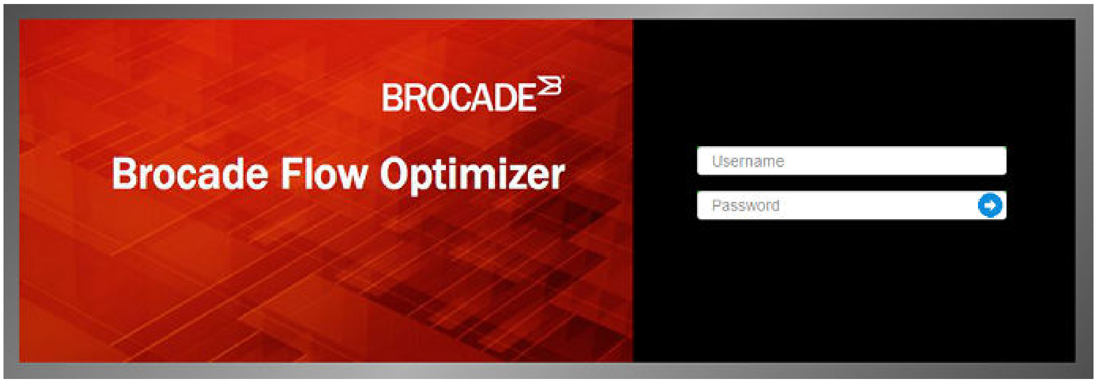
The Login page is used to login to the Brocade Flow Optimizer application on the host server that is running the application. The application must be running to login. If it is not running, you must start the application before you login.

Once you login, the application session starts. If there is no user activity for 30 minutes after the session starts, the session times out (closes), and you must login again.

To login, open your browser and point it to **https://<Server_IP>:8089**.

NOTE
The port number must be 8089.

The Login page appears.



Type your username and password in the appropriate boxes, then press **Enter** or click the **blue arrow**.

The Dashboard page appears.

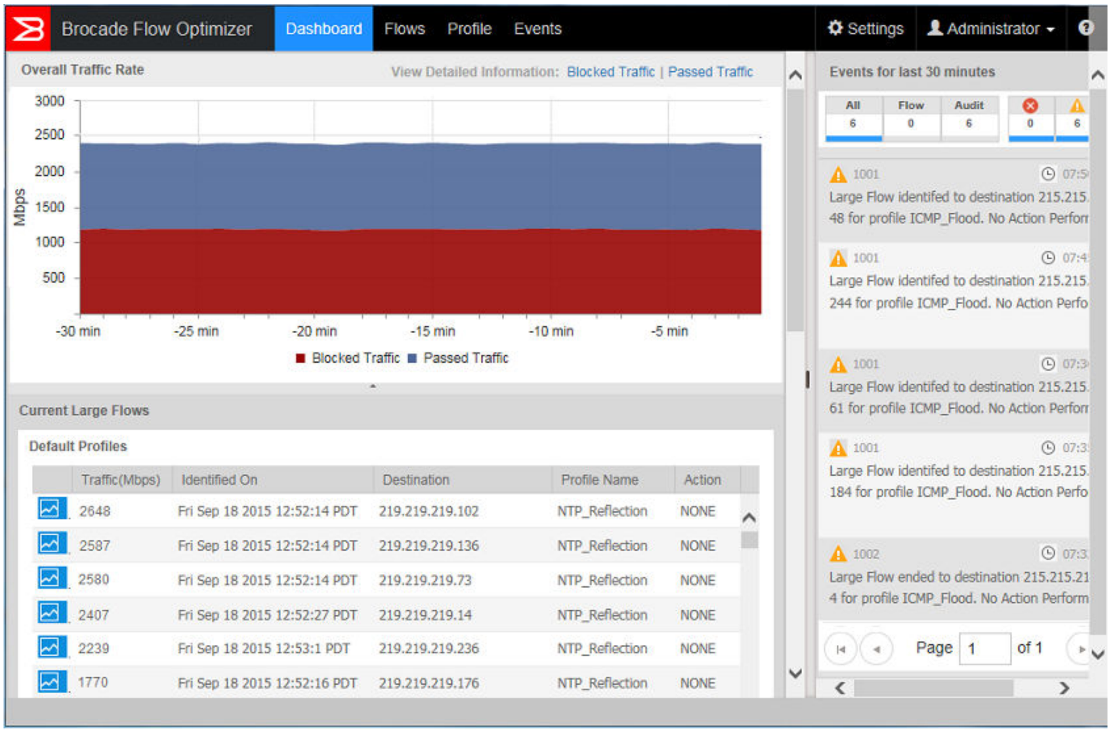
Dashboard Page

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.

The following figure shows the Dashboard page.



Current Large Flows

Default Profiles

	Traffic(Mbps)	Identified On	Destination	Profile Name	Action
	2648	Fri Sep 18 2015 12:52:14 PDT	219.219.219.102	NTP_Reflection	NONE
	2587	Fri Sep 18 2015 12:52:14 PDT	219.219.219.136	NTP_Reflection	NONE
	2580	Fri Sep 18 2015 12:52:14 PDT	219.219.219.73	NTP_Reflection	NONE
	2407	Fri Sep 18 2015 12:52:27 PDT	219.219.219.14	NTP_Reflection	NONE
	2239	Fri Sep 18 2015 12:53:1 PDT	219.219.219.236	NTP_Reflection	NONE
	1770	Fri Sep 18 2015 12:52:16 PDT	219.219.219.176	NTP_Reflection	NONE

1001 07:5
Large Flow identifed to destination 215.215.
48 for profile ICMP_Flood. No Action Perforr

1001 07:4
Large Flow identifed to destination 215.215.
244 for profile ICMP_Flood. No Action Perfo

1001 07:3
Large Flow identifed to destination 215.215.
61 for profile ICMP_Flood. No Action Perforr

1001 07:3
Large Flow identifed to destination 215.215.
184 for profile ICMP_Flood. No Action Perfo

1002 07:3
Large Flow ended to destination 215.215.21
4 for profile ICMP_Flood. No Action Perform

For information on the Overall Traffic Rate graph, the Current Large Flows tables, and the Events pane, see:

- Overall Traffic Rate on page 73
- Current Large Flows on page 76
- Events Pane on page 78

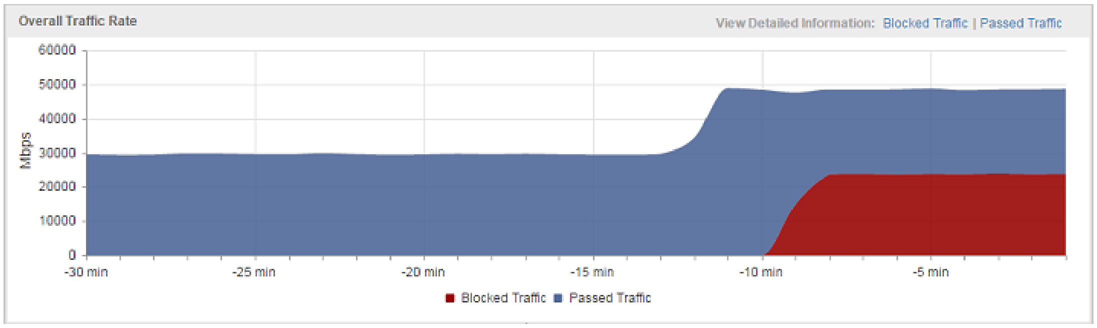
Overall Traffic Rate

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 following figure shows the Overall Traffic Rate graph.



The meaning of blocked and passed traffic are:

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.

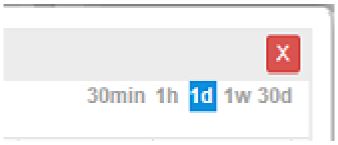
The dialog shows large flows (flows that exceed profile thresholds) that are being dropped. The mitigation actions defined in the profiles used to monitor the traffic are actions that result in the traffic being dropped.

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:

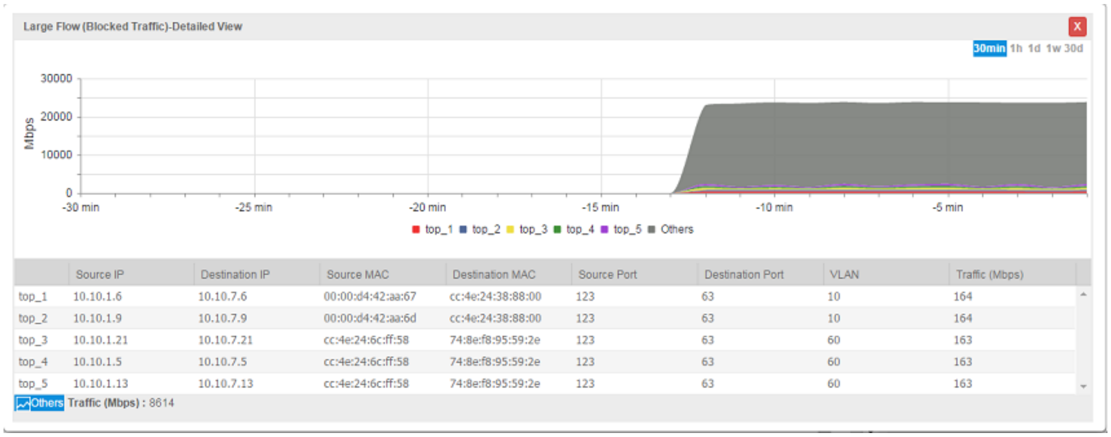
- **1h:** Click this label to view data for the last hour.
- **1d:** Click this label to view data for the last day.
- **1w:** Click this label to view data for the last week.
- **30d:** Click this label to view data for the 30 days.

The labels are:



(In the example above, one day is selected. The default is 30 minutes.)

The following figure shows data collected on all large flows that have been blocked over the 30 minutes.


Large Flow (Blocked Traffic)-Detailed View

	Source IP	Destination IP	Source MAC	Destination MAC	Source Port	Destination Port	VLAN	Traffic (Mbps)
top_1	10.10.1.6	10.10.7.6	00:00:d4:42:aa:67	cc:4e:24:38:88:00	123	63	10	164
top_2	10.10.1.9	10.10.7.9	00:00:d4:42:aa:6d	cc:4e:24:38:88:00	123	63	10	164
top_3	10.10.1.21	10.10.7.21	cc:4e:24:6c:ff:58	74:8e:f8:95:59:2e	123	63	60	163
top_4	10.10.1.5	10.10.7.5	cc:4e:24:6c:ff:58	74:8e:f8:95:59:2e	123	63	60	163
top_5	10.10.1.13	10.10.7.13	cc:4e:24:6c:ff:58	74:8e:f8:95:59:2e	123	63	60	163

Others Traffic (Mbps) : 8614

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.

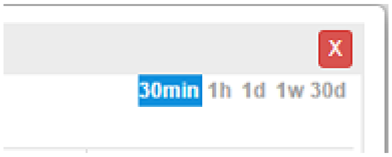
The dialog shows large flows (flows that exceed profile thresholds) that are not being dropped. The mitigation actions defined in the profiles used to monitor the traffic are not actions that result in the traffic being dropped.

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:

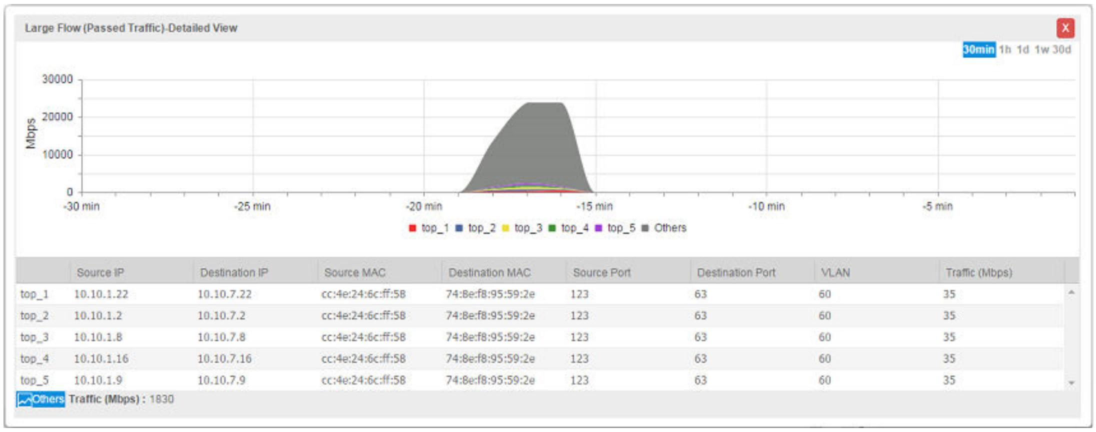
- **1h:** Click this label to view data for the last hour.
- **1d:** Click this label to view data for the last day.
- **1w:** Click this label to view data for the last week.
- **30d:** Click this label to view data for the 30 days.

The labels are:



(In the example above, 30 minutes is selected, which is the default.)

The following figure shows data collected on all large flows that have been passed through the system over the last 30 minutes.



	Source IP	Destination IP	Source MAC	Destination MAC	Source Port	Destination Port	VLAN	Traffic (Mbps)
top_1	10.10.1.22	10.10.7.22	cc:4e:24:6c:ff:58	74:8e:f8:95:59:2e	123	63	60	35
top_2	10.10.1.2	10.10.7.2	cc:4e:24:6c:ff:58	74:8e:f8:95:59:2e	123	63	60	35
top_3	10.10.1.8	10.10.7.8	cc:4e:24:6c:ff:58	74:8e:f8:95:59:2e	123	63	60	35
top_4	10.10.1.16	10.10.7.16	cc:4e:24:6c:ff:58	74:8e:f8:95:59:2e	123	63	60	35
top_5	10.10.1.9	10.10.7.9	cc:4e:24:6c:ff:58	74:8e:f8:95:59:2e	123	63	60	35

Others Traffic (Mbps) : 1830

The following table lists the columns in the Large Flow (Passed 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).

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.)

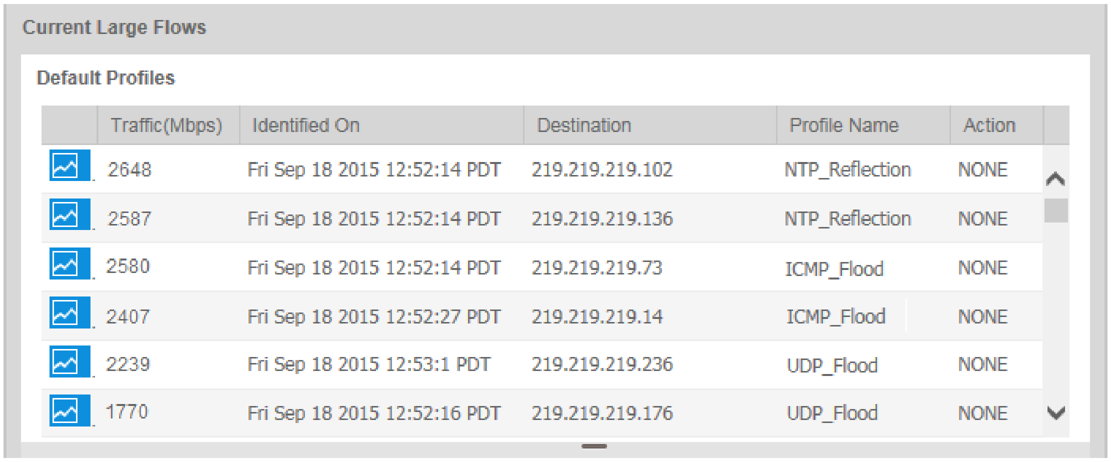
NOTE
Each table lists the large flows that have the highest bandwidth utilization (as Mbps). The maximum number of flows that can be listed in the Current Large Flows tables is 50.

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 following figure shows the Current Large Flows table for Default profiles.



Current Large Flows

Default Profiles

	Traffic(Mbps)	Identified On	Destination	Profile Name	Action
📈	2648	Fri Sep 18 2015 12:52:14 PDT	219.219.219.102	NTP_Reflection	NONE
📈	2587	Fri Sep 18 2015 12:52:14 PDT	219.219.219.136	NTP_Reflection	NONE
📈	2580	Fri Sep 18 2015 12:52:14 PDT	219.219.219.73	ICMP_Flood	NONE
📈	2407	Fri Sep 18 2015 12:52:27 PDT	219.219.219.14	ICMP_Flood	NONE
📈	2239	Fri Sep 18 2015 12:53:1 PDT	219.219.219.236	UDP_Flood	NONE
📈	1770	Fri Sep 18 2015 12:52:16 PDT	219.219.219.176	UDP_Flood	NONE

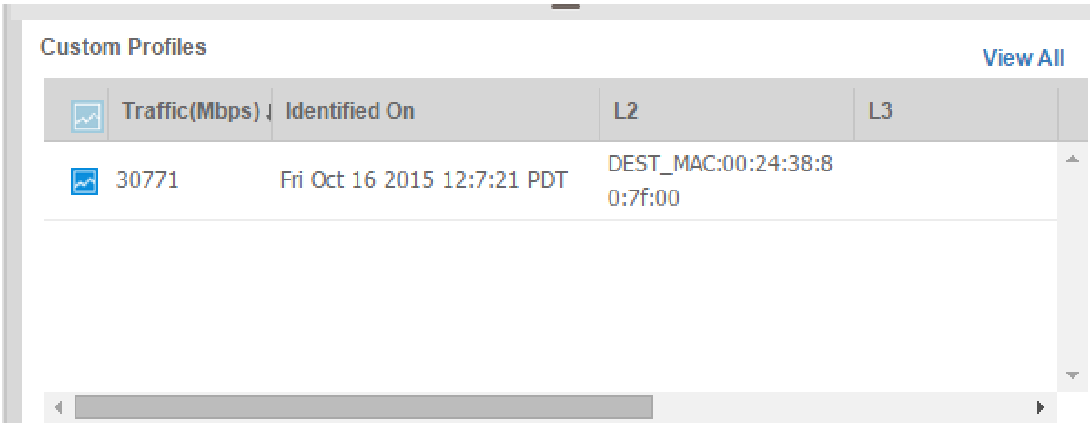
The columns in this table are:

- **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 following figure shows the Current Large Flows table for Custom profiles.



Custom Profiles

View All

	Traffic(Mbps) ↓	Identified On	L2	L3
	30771	Fri Oct 16 2015 12:7:21 PDT	DEST_MAC:00:24:38:8 0:7f:00	

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.

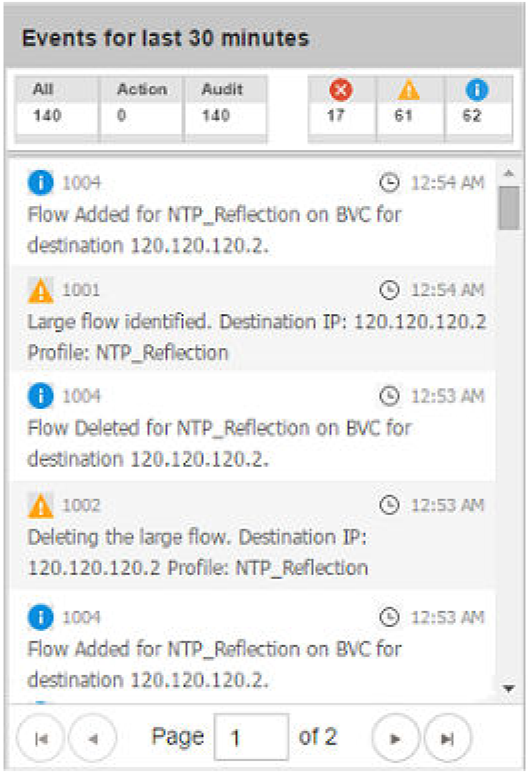
Events Pane

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.

The following figure shows the Events pane.



Events for last 30 minutes

All	Action	Audit	✖	⚠	ℹ
140	0	140	17	61	62

ℹ 1004 12:54 AM
Flow Added for NTP_Reflection on BVC for destination 120.120.120.2.

⚠ 1001 12:54 AM
Large flow identified. Destination IP: 120.120.120.2 Profile: NTP_Reflection

ℹ 1004 12:53 AM
Flow Deleted for NTP_Reflection on BVC for destination 120.120.120.2.

⚠ 1002 12:53 AM
Deleting the large flow. Destination IP: 120.120.120.2 Profile: NTP_Reflection

ℹ 1004 12:53 AM
Flow Added for NTP_Reflection on BVC for destination 120.120.120.2.

Page 1 of 2

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.

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	All the traffic flows received by the Brocade Flow Optimizer server that: • 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	All the traffic flows received by the Brocade Flow Optimizer server that: • 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	All the flows created by Brocade Flow Optimizer administrators. These are custom, user-defined flows created using the available network attributes or parameters and mitigation actions. This includes flows that are: • Created from learned flows using options provided in the Learned Flows tab. • Created by adding new flows using the Add Custom Flow option (click the **Create Flow** button to access the Add Custom Flow option).

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.

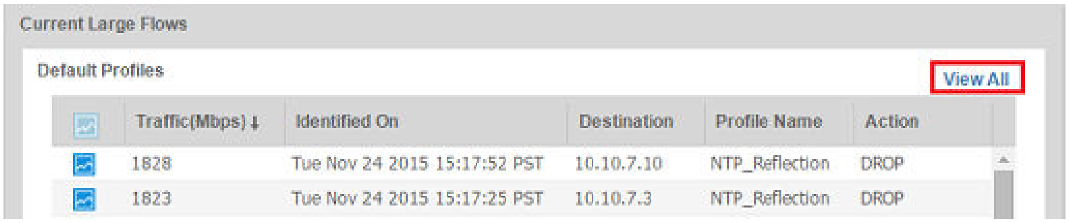
Navigation and refresh

You can navigate to the tab from the Dashboard by doing either of the following:

- Directly

  (Select the **Flows page**, then click the **Learned & Programmed Flows** tab.)
- From the Top 50 current Large Flows table of the Dashboard

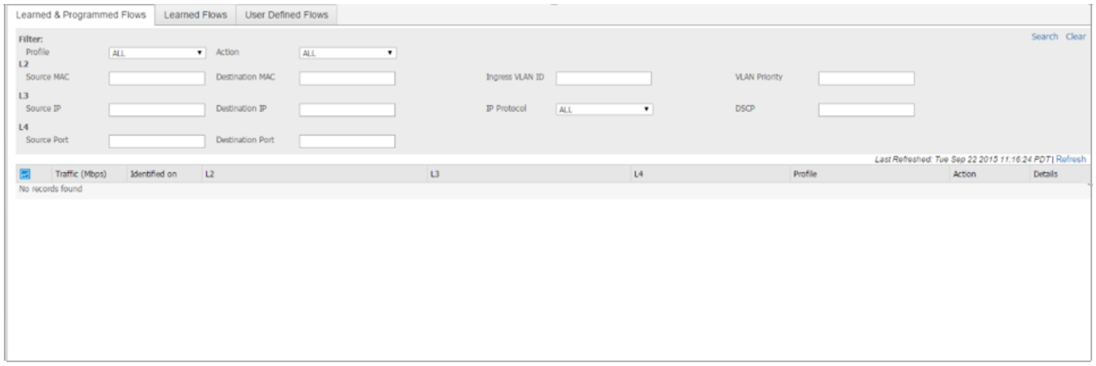
  (Click the **View All** option.)



	Traffic(Mbps) ↓	Identified On	Destination	Profile Name	Action
📈	1828	Tue Nov 24 2015 15:17:52 PST	10.10.7.10	NTP_Reflection	DROP
📈	1823	Tue Nov 24 2015 15:17:25 PST	10.10.7.3	NTP_Reflection	DROP

You are automatically redirected to the Learned & Programmed Flows tab. This page is not automatically refreshed. Click **Refresh** to view the latest set of active large flows.

This following figure shows the Learned & Programmed Flows tab.



Filter:
Profile ALL ▾ Action ALL ▾
L2
Source MAC Destination MAC Ingress VLAN ID VLAN Priority
L3
Source IP Destination IP IP Protocol ALL ▾ DSCP
L4
Source Port Destination Port

Last Refreshed: Tue Sep 22 2015 11:16:24 PDT | Refresh

📈	Traffic (Mbps)	Identified on	L2	L3	L4	Profile	Action	Details
No records found								

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.

The 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.

📈	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 action defined in the profile that is associated with the flow.
Details	Opens the Details view of the flow. Use this option to view more detailed information about the flow and to see if the flow is a composite flow (comprised of one or more flows).

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

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.

NOTE
To discover flows using filter criteria, use the steps in Discovering Large Flows by Inspecting Flows in the List on page 84.

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. Select one or more of the following filter items:

Option	Description
Option	**Description**
Profile	The name of the profile. Do one of the following: • Select one of the profiles in the list. • Select ALL to include all current profiles in the search.
L2 Source MAC	Type the source MAC address you want to include in your search. Flows of IP packets that have this address are included in the search results.
L3 Source IP	Type the source IP address you want to include in your search. Flows of IP packets that have this address are included in the search results.
L4 Source Port	Type the source port number you want to include in your search. Flows of IP packets that have this port number are included in the search results.
Action	The name of the mitigation action defined in the profile associated with the flow. Do one of the following: • Select one of the mitigation actions in the list. • Select ALL to include all current mitigation actions in the search.
L2 Destination MAC	Type the destination MAC address you want to include in your search. Flows of IP packets that have this address are included in the search results.
L3 Destination IP	Type the destination IP address you want to include in your search. Flows of IP packets that have this address are included in the search results.
L4 Destination Port	Type the destination port number you want to include in your search. Flows of IP packets that have this port number are included in the search results.
Ingress VLAN ID	Type the ingress VLAN ID you want to include in your search. Flows of IP packets received by the Brocade Flow Optimizer server that have this VLAN ID are included in the search results.

Option	Description
IP Protocol	The IP protocol (or protocols) you want to include in your search. Flows of IP packets that use the selected protocols are included in the search. Do one of the following: • Select one of the IP protocols. • Select ALL to include all IP protocols in the search.
VLAN Priority	Type the VLAN priority value you want to include in your search. The range of possible values is from 1 to 7. Flows of IP packets that have this value are included in the search results.
DSCP	Type the DSCP drop-precedence value you to include in your search. Flows of IP packets that have this value in the IP header are included in the search results.

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.

NOTE
To discover flows using filter criteria, use the steps in Discovering Large Flows Using Filter Criteria on page 83.

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

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. Scan the list of flows to find a flow you want to inspect.
4. Click the **Details** 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.

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

Learned Flows Tab

This tab lists of **all** of the traffic flows learned from sFlows received by the Brocade Flow Optimizer server. You use this tab to discover flows that have not been detected as large flows that are not listed in other system components. You can also use it to create custom flows from the flows you discover.

Learned flows can be:

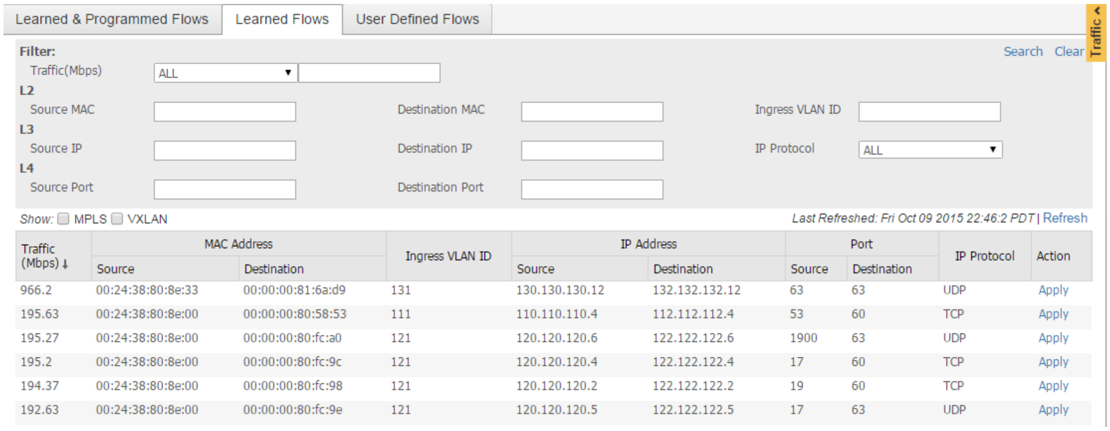
- Flows that are being monitored using profiles, but have not exceeded the large flow detection criteria of the profile associated with the flow.
- Flows on the network that are not being monitored using profiles.

Navigation and refresh

You can navigate to the tab from the Dashboard by selecting the **Flows page**, then click the **Learned Flows** tab.

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.

This following figure shows the Learned Flows tab.



Filter:

Traffic(Mbps) ALL ▾

L2

Source MAC

Destination MAC

Ingress VLAN ID

L3

Source IP

Destination IP

IP Protocol ALL ▾

L4

Source Port

Destination Port

Show: □ MPLS □ VXLAN

Last Refreshed: Fri Oct 09 2015 22:46:2 PDT | Refresh

Traffic (Mbps) ↓	MAC Address		Ingress VLAN ID	IP Address		Port		IP Protocol	Action
	Source	Destination		Source	Destination	Source	Destination		
966.2	00:24:38:80:8e:33	00:00:00:81:6a:d9	131	130.130.130.12	132.132.132.12	63	63	UDP	Apply
195.63	00:24:38:80:8e:00	00:00:00:80:58:53	111	110.110.110.4	112.112.112.4	53	60	TCP	Apply
195.27	00:24:38:80:8e:00	00:00:00:80:fc:a0	121	120.120.120.6	122.122.122.6	1900	63	UDP	Apply
195.2	00:24:38:80:8e:00	00:00:00:80:fc:9c	121	120.120.120.4	122.122.122.4	17	60	TCP	Apply
194.37	00:24:38:80:8e:00	00:00:00:80:fc:98	121	120.120.120.2	122.122.122.2	19	60	TCP	Apply
192.63	00:24:38:80:8e:00	00:00:00:80:fc:9e	121	120.120.120.5	122.122.122.5	17	63	UDP	Apply

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.

The 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.

NOTE
The table provides the same information about the large flows that is provided in the table in the Dashboard.

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

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. Select one or more of the following filter items:

Option	Description
Option	**Description**
Traffic (Mbps)	Type the source MAC address you want to include in your search. Flows of IP packets that have this address are included in the search results.
L2 Source MAC	Type the source MAC address you want to include in your search. Flows of IP packets that have this address are included in the search results.
L3 Source IP	Type the source IP address you want to include in your search. Flows of IP packets that have this address are included in the search results.
L4 Source Port	Type the source port number you want to include in your search. Flows of IP packets that have this port number are included in the search results.
Action	The name of the mitigation action defined in the profile associated with the flow. Do one of the following: • Select one of the mitigation actions in the list. • Select ALL to include all current mitigation actions in the search.
L2 Destination MAC	Type the destination MAC address you want to include in your search. Flows of IP packets that have this address are included in the search results.
L3 Destination IP	Type the destination IP address you want to include in your search. Flows of IP packets that have this address are included in the search results.
L4 Destination Port	Type the destination port number you want to include in your search. Flows of IP packets that have this port number are included in the search results.
Ingress VLAN ID	Type the ingress VLAN ID you want to include in your search. Flows of IP packets received by the Brocade Flow Optimizer server that have this VLAN ID are included in the search results.
IP Protocol	The IP protocol (or protocols) you want to include in your search. Flows of IP packets that use the selected protocols are included in the search. Do one of the following: • Select one of the IP protocols. • Select ALL to include all IP protocols in the search.

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.

User Defined Flows Tab

This tab lists **all** of the current custom (user-defined) flows. You use this tab to discover user-defined flows that are not listed in other system components. You can also use it to open the Add Custom Flow dialog, which you use to create custom flows.

Network flows that have the same network attributes as the user-defined flow are shown in the table below the filtering options.

Navigation and refresh

You can navigate to the tab from the Dashboard by selecting the **Flows page**, then click the **User Defined Flows** tab.

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

This following figure shows the User Defined Flows tab.

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.

The 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.

📈	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 action defined in the profile that is associated with the flow.
Details	Opens the Details view of the flow. Use this option to view more detailed information about the flow and to see if the flow is a composite flow (comprised of one or more flows).

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

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), 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 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. Select one or more of the following filter items:

Option	Description
Option	**Description**
Hide Learned Flows	Select the option if you do not want learned flows to be included in the search results.
L2 Source MAC	Type the source MAC address you want to include in your search. Flows of IP packets that have this address are included in the search results.

Option	Description
L3 Source IP	Type the source IP address you want to include in your search. Flows of IP packets that have this address are included in the search results.
L4 Source Port	Type the source port number you want to include in your search. Flows of IP packets that have this port number are included in the search results.
Priority	Type the flow priority you want to include in your search. Flows that have this priority are included in the search results.
L2 Destination MAC	Type the destination MAC address you want to include in your search. Flows of IP packets that have this address are included in the search results.
L3 Destination IP	Type the destination IP address you want to include in your search. Flows of IP packets that have this address are included in the search results.
L4 Destination Port	Type the destination port number you want to include in your search. Flows of IP packets that have this port number are included in the search results.
Ingress VLAN ID	Type the ingress VLAN ID you want to include in your search. Flows of IP packets received by the Brocade Flow Optimizer server that have this VLAN ID are included in the search results.
IP Protocol	The IP protocol (or protocols) you want to include in your search. Flows of IP packets that use the selected protocols are included in the search. Do one of the following: • Select one of the IP protocols. • Select ALL to include all IP protocols in the search.
VLAN Priority	Type the VLAN priority value you want to include in your search. The range of possible values is from 1 to 7. Flows of IP packets that have this value are included in the search results.
DSCP	Type the DSCP drop-precedence value you to include in your search. Flows of IP packets that have this value in the IP header are included in the search results.

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.

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:

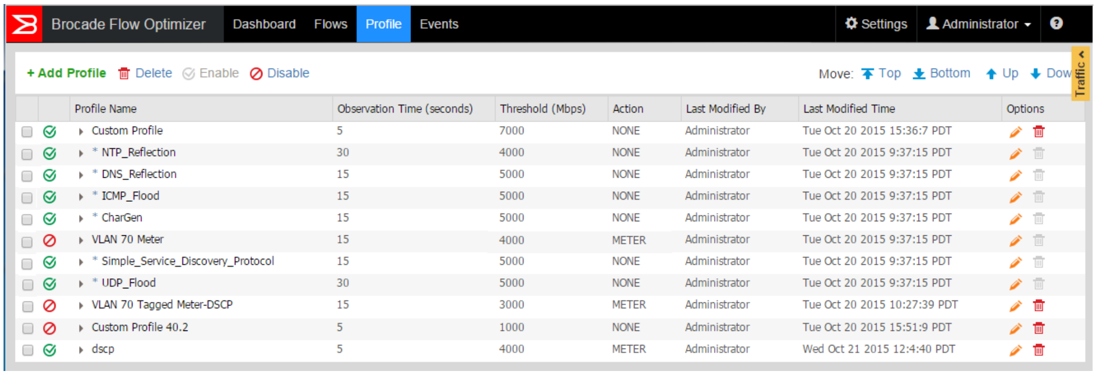
- View basic information about a profile, such as the name, large flow detection parameters, and mitigation action.
- View detailed information about a profile (click the arrow button next to the profile name).
- Enable, disable, or delete profiles.
- Open the dialogs used to create new Custom profiles 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.

The following figure shows the Profile page. In this example, Both Default profiles and Custom profiles are shown. Some of the profiles are enable, and some are disabled (indicated by the icon at the left side of the table).



		Profile Name	Observation Time (seconds)	Threshold (Mbps)	Action	Last Modified By	Last Modified Time	Options
□	✓	Custom Profile	5	7000	NONE	Administrator	Tue Oct 20 2015 15:36:7 PDT	
□	✓	* NTP_Reflection	30	4000	NONE	Administrator	Tue Oct 20 2015 9:37:15 PDT	
□	✓	* DNS_Reflection	15	5000	NONE	Administrator	Tue Oct 20 2015 9:37:15 PDT	
□	✓	* ICMP_Flood	15	5000	NONE	Administrator	Tue Oct 20 2015 9:37:15 PDT	
□	✓	* CharGen	15	5000	NONE	Administrator	Tue Oct 20 2015 9:37:15 PDT	
□	⊘	VLAN 70 Meter	15	4000	METER	Administrator	Tue Oct 20 2015 9:37:15 PDT	
□	✓	* Simple_Service_Discovery_Protocol	15	5000	NONE	Administrator	Tue Oct 20 2015 9:37:15 PDT	
□	✓	* UDP_Flood	30	5000	NONE	Administrator	Tue Oct 20 2015 9:37:15 PDT	
□	⊘	VLAN 70 Tagged Meter-DSCP	15	3000	METER	Administrator	Tue Oct 20 2015 10:27:39 PDT	
□	⊘	Custom Profile 40.2	5	1000	NONE	Administrator	Tue Oct 20 2015 15:51:9 PDT	
□	✓	dscp	5	4000	METER	Administrator	Wed Oct 21 2015 12:4:40 PDT	

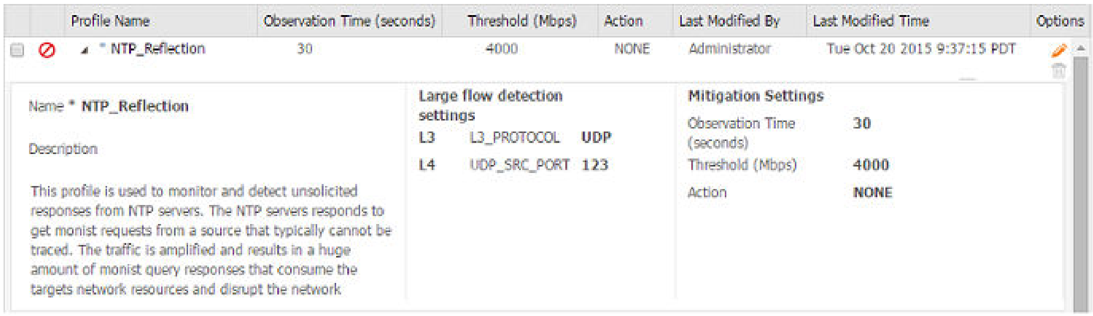
Viewing profile details

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.

The following figure shows the expanded view for a profile named NTP Reflection. This view shows the profile name and description, the settings for all of the profile parameters, and the last time it was modified. The values shown are the current specified values for the profile.



		Profile Name	Observation Time (seconds)	Threshold (Mbps)	Action	Last Modified By	Last Modified Time	Options
□	⊘	* NTP_Reflection	30	4000	NONE	Administrator	Tue Oct 20 2015 9:37:15 PDT	

Name * NTP_Reflection

Description

This profile is used to monitor and detect unsolicited responses from NTP servers. The NTP servers responds to get monist requests from a source that typically cannot be traced. The traffic is amplified and results in a huge amount of monist query responses that consume the targets network resources and disrupt the network

Large flow detection settings

L3	L3_PROTOCOL	UDP
L4	UDP_SRC_PORT	123

Mitigation Settings

Observation Time (seconds)	30
Threshold (Mbps)	4000
Action	NONE

Enabling and disabling profiles

You can easily enable or disable profiles directly from the Profile page. You have two basic options for enabling or disabling profiles. You can enable or disable individual profiles (one profile at a time), or you can enable or disable multiple profiles at the same time. Profiles that have a green checkmark are currently enabled: profiles with a red checkmark are currently disabled.

To enable or disable one or more profiles, do the following:

1. Click the **checkbox** next to each profile you want to enable or disable.
2. Do one of the following:
   - Click the **Enable** option above the table. All the profiles you selected are now enabled.
   - Click the **Disable** option above the table. All the profiles you selected are now disabled.

NOTE
The system automatically ignores invalid selections. For example, if you accidentally select profiles that are already enabled before clicking the **Enable** option, the system enables all profiles you selected that are disabled, and ignores invalid selections.

Changing the priority of a profile

The position or ranking of a profile in the list indicates the priority of the profile. The higher the position in the list, the higher the priority. The lower the position in the list, the lower the priority.

You have two basic options for changing the priority of a profile. You can make granular changes to the priority of a profile by moving it up or down in the list one row at a time. You can also change the priority of a profile to the highest or lowest possible priority by moving the profile to the top of the list (highest priority), or to the bottom of the list (lowest priority).

Granular changes	
To **increase** the priority	Click the **Move Up** button until the profile has the desired priority.
To **decrease** the priority	Click the **Move Down** button until the profile has the desired priority.
Change to the highest or lowest possible priority	
To change to the **highest** possible priority	Click the **Top** button.
To change to the **lowest** possible priority	Click the **Bottom** button.

Opening the dialogs used to add (create) or edit profiles

The dialogs you use to create new profiles and edit profiles can be opened directly from the Profiles page.

The two dialogs are:

- Add New Profile dialog (To open this dialog, click the **+Add Profile** link above the list of profiles.)
- Edit Profile dialog (To open this dialog, click the **pencil icon** in the Options column.)

Deleting profiles

You can delete profiles directly from the Profile page by clicking the **trash can** icon in the Options column.

NOTE
Make sure that you are aware of the consequences of deleting profiles.

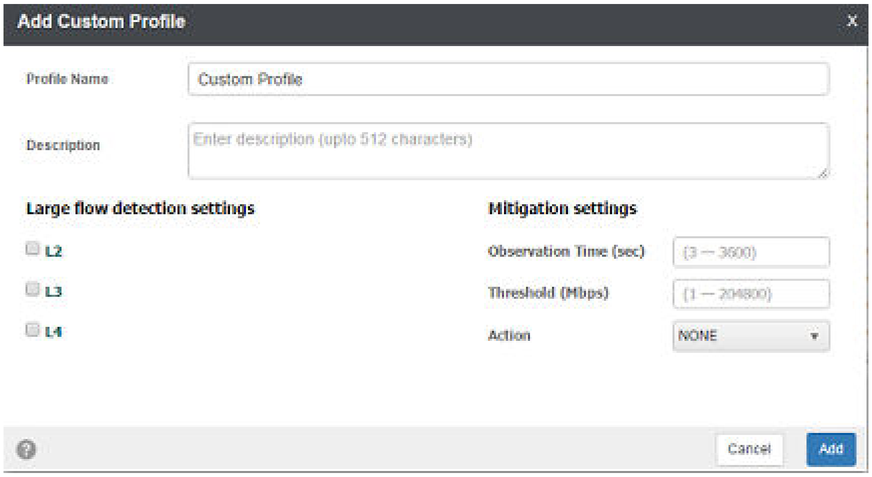
For more information on profiles, see the following:

- About Profiles on page 49
- Custom Profiles on page 51
- Default Profiles on page 49
- Edit Profile Dialog on page 92
- Enabling and Disabling Profiles on page 67
- Editing Profiles on page 62
- Large Flow Detection Parameters on page 52
- Profile Management on page 49

Add Custom Profile Dialog

You use the Add Custom Profile dialog to create new custom profiles. The dialog contains all of the options you need to configure the custom profile for use.

The following figure shows a blank Add Custom Profile dialog.



Add Custom Profile

Profile Name: Custom Profile

Description: Enter description (upto 512 characters)

Large flow detection settings

□ L2

□ L3

□ L4

Mitigation settings

Observation Time (sec): (3 — 3600)

Threshold (Mbps): (1 — 204800)

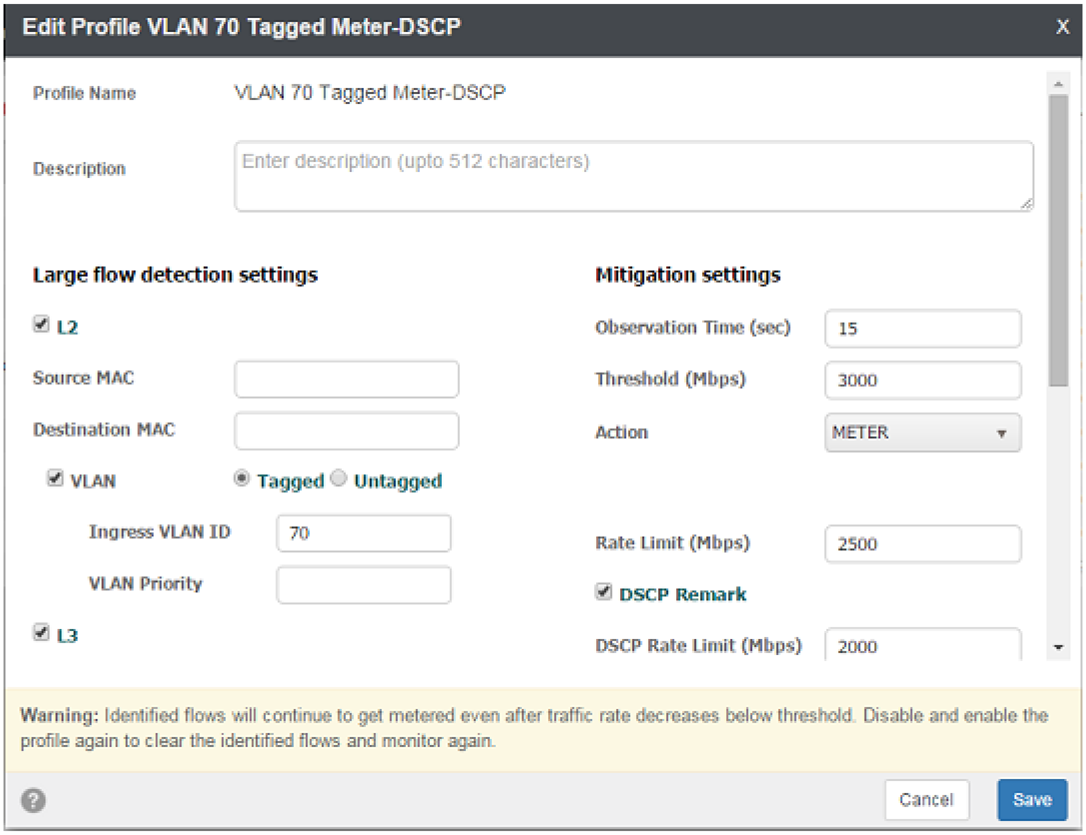
Action: NONE

Edit Profile Dialog

You use the Edit Profile dialog to edit existing profiles. The dialog contains all of the options you need to edit the profile as needed.

NOTE
You use this dialog to edit default profiles and custom profiles.

The following figure shows the Edit Profile dialog. In this example, the profile that has been selected for editing is the default profile named NTP_Reflection.



Edit Profile VLAN 70 Tagged Meter-DSCP

Profile Name: VLAN 70 Tagged Meter-DSCP

Description: Enter description (upto 512 characters)

Large flow detection settings

☑ L2

Source MAC:

Destination MAC:

☑ VLAN ● Tagged ○ Untagged

Ingress VLAN ID: 70

VLAN Priority:

☑ L3

Mitigation settings

Observation Time (sec): 15

Threshold (Mbps): 3000

Action: METER

Rate Limit (Mbps): 2500

☑ DSCP Remark

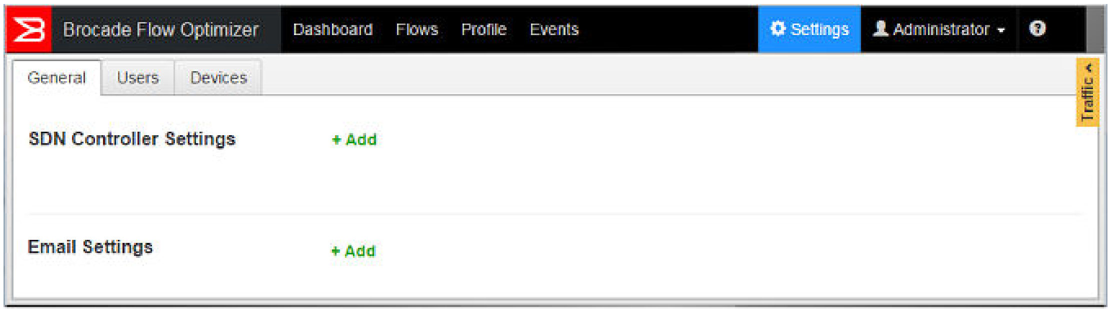
DSCP Rate Limit (Mbps): 2000

Warning: Identified flows will continue to get metered even after traffic rate decreases below threshold. Disable and enable the profile again to clear the identified flows and monitor again.

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.

The following figure shows the Settings page (the General tab is the default tab for this page). In this example, the SDN Controller settings and the email notification settings have not yet been configured.



SDN Controller Settings + Add

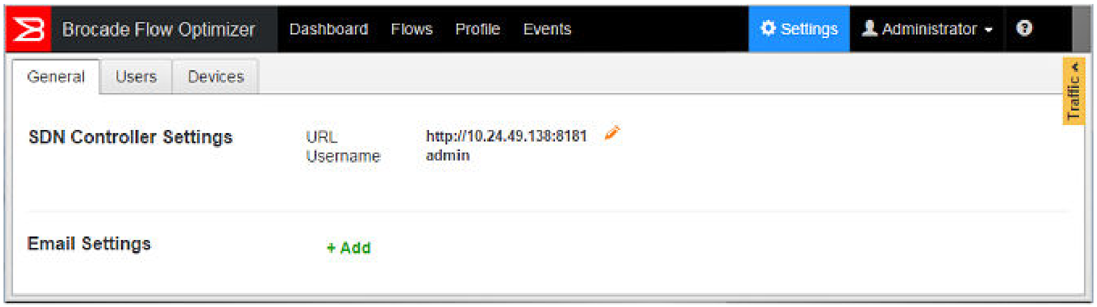
Email Settings + Add

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).

The following figure shows the General tab. In this example, the SDN Controller settings have been configured, and the email notification settings have not been configured.



SDN Controller Settings

URL http://10.24.49.138:8181

Username admin

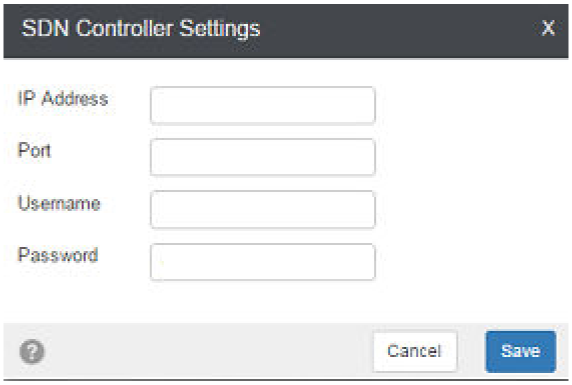
Email Settings

SDN Controller Settings Dialog

You 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. You set up the connection for the first time as part of the initial system configuration.

Configuring the settings involves specifying the IP address and REST API port number of the SDN Controller in the dialog.

The following figure shows the SDN Controller Settings dialog.



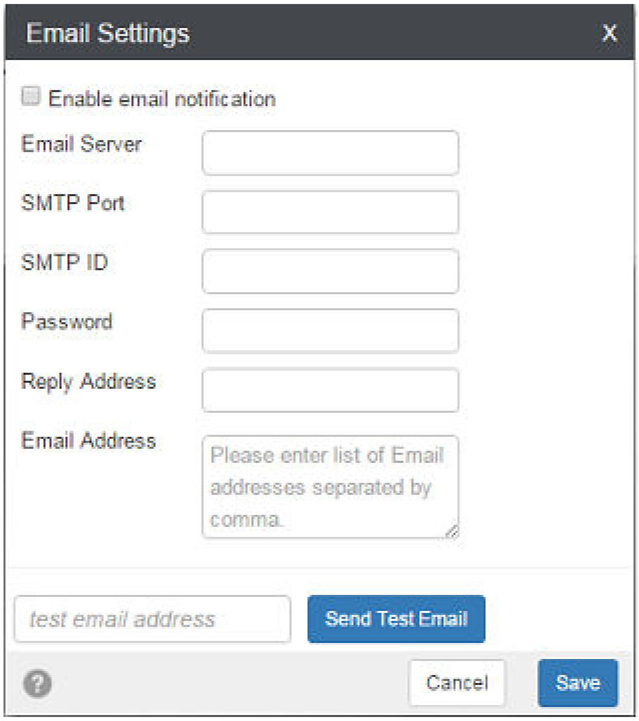
For detailed steps on using this dialog, see:

- Setting up the Connection to the SDN Controller on page 17
- Modifying or Re-entering the SDN Controller Settings on page 34

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.

The following figure shows the Email Settings dialog.



For detailed steps on using this dialog, see:

- Setting up or Editing Email Notifications on page 26

Users Tab

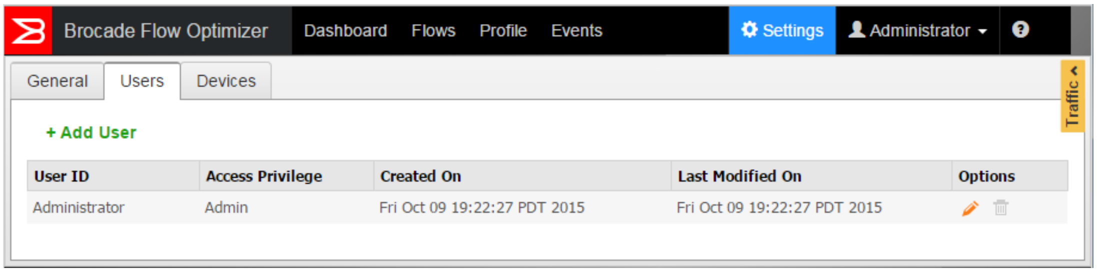
The Users tab shows the list of current system users, including the user role (Administrator or Operator) for each user. You use the tab to view the list of current users and to open the dialogs you use to manage users.

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

The following figure shows the Users tab. In this example, the only user is an Administrator.



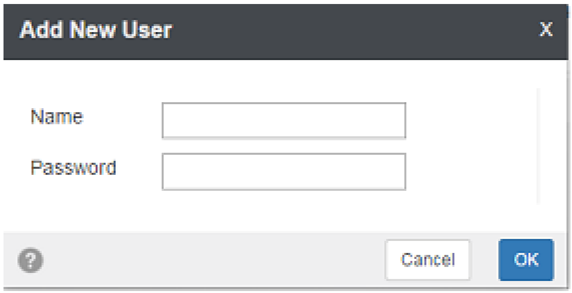
User ID	Access Privilege	Created On	Last Modified On	Options
Administrator	Admin	Fri Oct 09 19:22:27 PDT 2015	Fri Oct 09 19:22:27 PDT 2015	✎ 🗑

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.

The following figure shows the Add New User dialog.



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**.

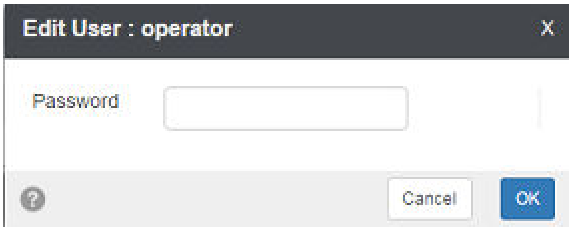
   The new user is added to the list of current users.

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 following figure shows the Edit User dialog.



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

Devices Tab

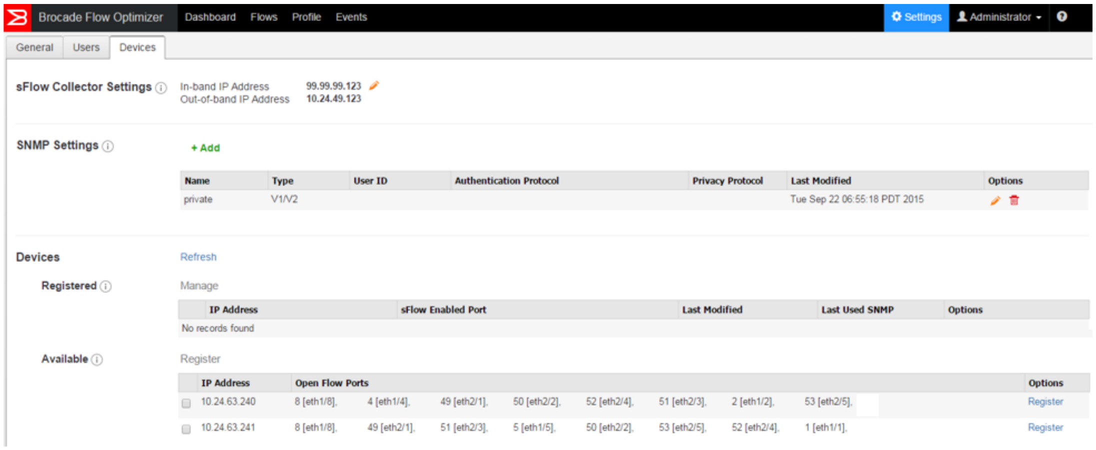
The Devices tab of the Settings page shows the current configuration of the system devices including the SNMP settings used for the communications between the Brocade Flow Optimizer and system devices. You use this tab to view the current device settings and SNMP communications settings.

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

The sections of the Devices tab are:

- sFlow Collector Settings
- SNMP Settings
- Devices

The following figure shows the Devices tab. In this example, sFlow Collector settings and SNMP settings exist, and devices have been added but not yet registered to forward sFlow samples.



sFlow Collector Settings

In-band IP Address 99.99.99.123
Out-of-band IP Address 10.24.49.123

SNMP Settings

+ Add

Name	Type	User ID	Authentication Protocol	Privacy Protocol	Last Modified	Options
private	V1/V2				Tue Sep 22 06:55:18 PDT 2015	

Devices

Refresh

Registered

Manage

	IP Address	sFlow Enabled Port	Last Modified	Last Used SNMP	Options
No records found					

Available

Register

	IP Address	Open Flow Ports	Options
□	10.24.63.240	8 [eth1/8], 4 [eth1/4], 49 [eth2/1], 50 [eth2/2], 52 [eth2/4], 51 [eth2/3], 2 [eth1/2], 53 [eth2/5],	Register
□	10.24.63.241	8 [eth1/8], 49 [eth2/1], 51 [eth2/3], 5 [eth1/5], 50 [eth2/2], 53 [eth2/5], 52 [eth2/4], 1 [eth1/1],	Register

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. You specify the sFlow destination IP addresses by selecting two IP addresses using the sFlow Collector Settings dialog.

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. You specify the options for the profiles using the SNMP Settings dialog.

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. The following table describes the Registered table and Available tables in the Devices section of the Devices tab.

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. You can delete devices from this list so that they are no longer a registered device and cannot forward sFlow samples. Once you delete a device from this list, it is automatically moved to the list of available devices (shown in the Available table).

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

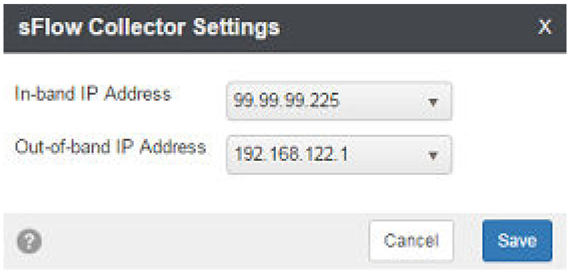
It is important that you maintain these lists to ensure they are current. Maintaining the lists is one of the key device management tasks.

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.

The following figure shows the sFlow Collector dialog.



sFlow Collector Settings

In-band IP Address: 99.99.99.225

Out-of-band IP Address: 192.168.122.1

For detailed steps on using this dialog, see:

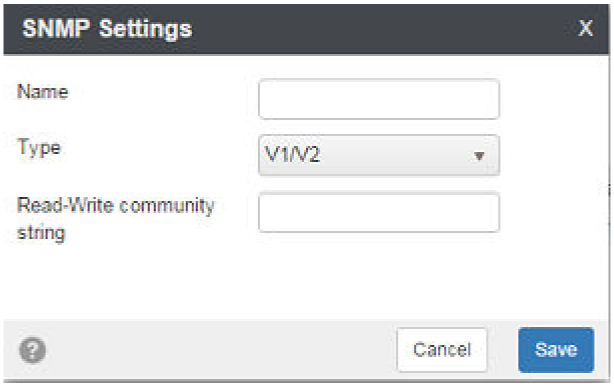
- Configuring the sFlow Collector Settings on page 19
- Modifying or Re-entering the SDN Controller Settings on page 34

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).

The following figure shows the SNMP Settings dialog. In this example, v1/v2 is selected (the default).



SNMP Settings

Name

Type: V1/V2

Read-Write community string

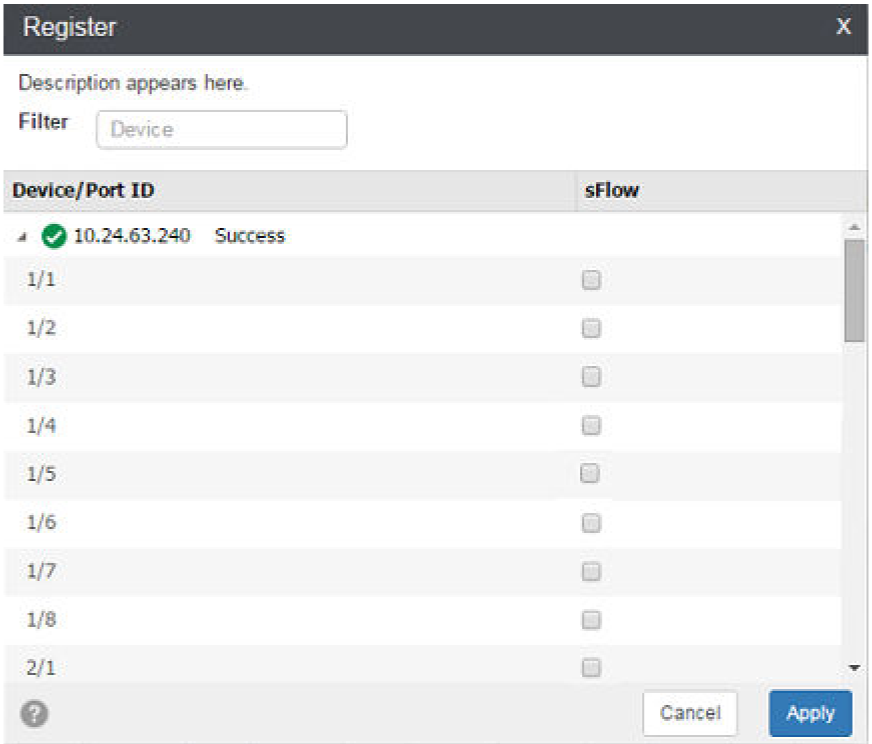
For detailed steps on using this dialog, see:

- Configuring SNMP Communication Settings on page 20
- Editing v1/v2 SNMP Profiles on page 35
- Editing v3 SNMP Profiles on page 36

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.

The following figure shows the Register dialog. In this example, a device is being registered to forward sFlow samples. No ports have yet been selected (enabled) to forward sFlows).



Register

Description appears here.

Filter: Device

Device/Port ID	sFlow
✓ 10.24.63.240 Success	
1/1	□
1/2	□
1/3	□
1/4	□
1/5	□
1/6	□
1/7	□
1/8	□
2/1	□

For detailed steps on using this dialog, see:

- Registering Devices on page 40
- Unregistering Devices on page 41
- Managing Registered Devices on page 42

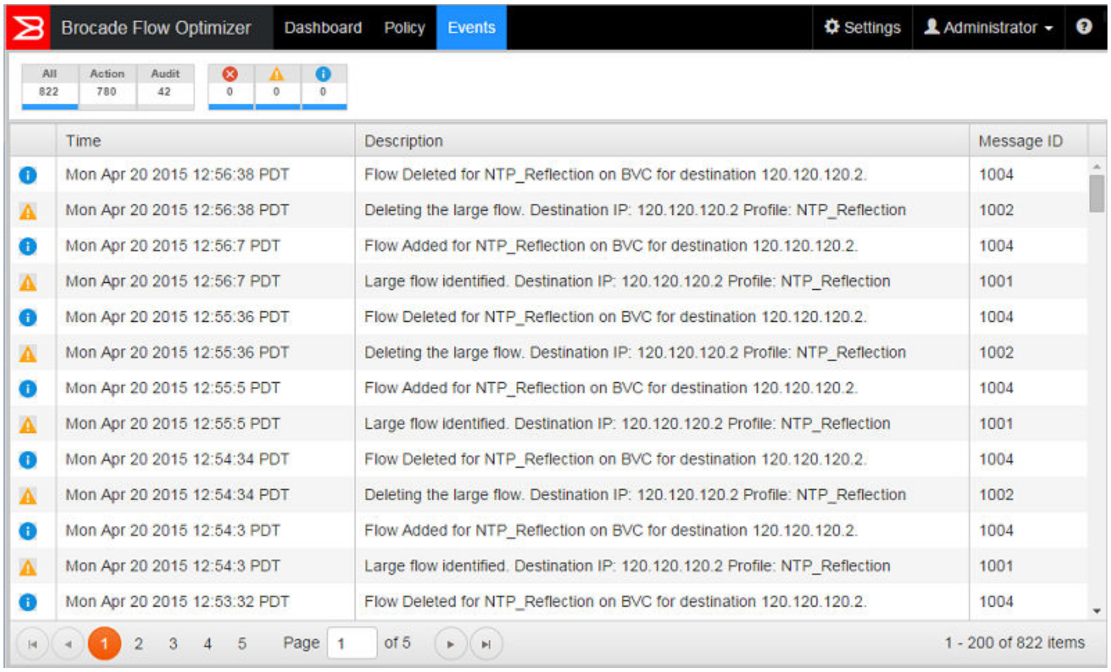
Events Page

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.

The following figure shows the Events page.



	Time	Description	Message ID
ⓘ	Mon Apr 20 2015 12:56:38 PDT	Flow Deleted for NTP_Reflection on BVC for destination 120.120.120.2.	1004
⚠	Mon Apr 20 2015 12:56:38 PDT	Deleting the large flow. Destination IP: 120.120.120.2 Profile: NTP_Reflection	1002
ⓘ	Mon Apr 20 2015 12:56:7 PDT	Flow Added for NTP_Reflection on BVC for destination 120.120.120.2.	1004
⚠	Mon Apr 20 2015 12:56:7 PDT	Large flow identified. Destination IP: 120.120.120.2 Profile: NTP_Reflection	1001
ⓘ	Mon Apr 20 2015 12:55:36 PDT	Flow Deleted for NTP_Reflection on BVC for destination 120.120.120.2.	1004
⚠	Mon Apr 20 2015 12:55:36 PDT	Deleting the large flow. Destination IP: 120.120.120.2 Profile: NTP_Reflection	1002
ⓘ	Mon Apr 20 2015 12:55:5 PDT	Flow Added for NTP_Reflection on BVC for destination 120.120.120.2.	1004
⚠	Mon Apr 20 2015 12:55:5 PDT	Large flow identified. Destination IP: 120.120.120.2 Profile: NTP_Reflection	1001
ⓘ	Mon Apr 20 2015 12:54:34 PDT	Flow Deleted for NTP_Reflection on BVC for destination 120.120.120.2.	1004
⚠	Mon Apr 20 2015 12:54:34 PDT	Deleting the large flow. Destination IP: 120.120.120.2 Profile: NTP_Reflection	1002
ⓘ	Mon Apr 20 2015 12:54:3 PDT	Flow Added for NTP_Reflection on BVC for destination 120.120.120.2.	1004
⚠	Mon Apr 20 2015 12:54:3 PDT	Large flow identified. Destination IP: 120.120.120.2 Profile: NTP_Reflection	1001
ⓘ	Mon Apr 20 2015 12:53:32 PDT	Flow Deleted for NTP_Reflection on BVC for destination 120.120.120.2.	1004

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

ℹ	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.

Troubleshooting

There are some basic procedures you can use to resolve issues you may encounter with the Brocade Flow Optimizer application database.

The troubleshooting steps cover these scenarios:

- If PostgreSQL Installed on Ubuntu on page 103
- If dbinitialization is triggered with permission denied error on page 103

NOTE
If you need to contact Support, make sure you have all the information you need to provide to Support (see The Process for Contacting Support on page 104).

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>/.

The Process for Contacting Support

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

The tasks are:

- (Optional) Changing the Logging Level on page 104
- Generating Support Save Data on page 105
- Collecting Information to Report an Issue to Support on page 105

Changing the Logging Level

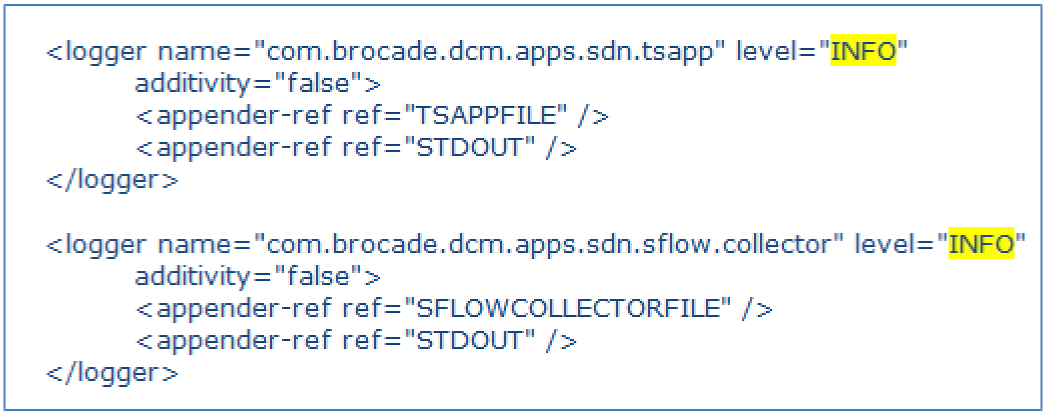
When you report an issue to Support, you can enable the logging of debug messages by changing the logging level from INFO (logging of information) to DEBUG (debugging).

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:

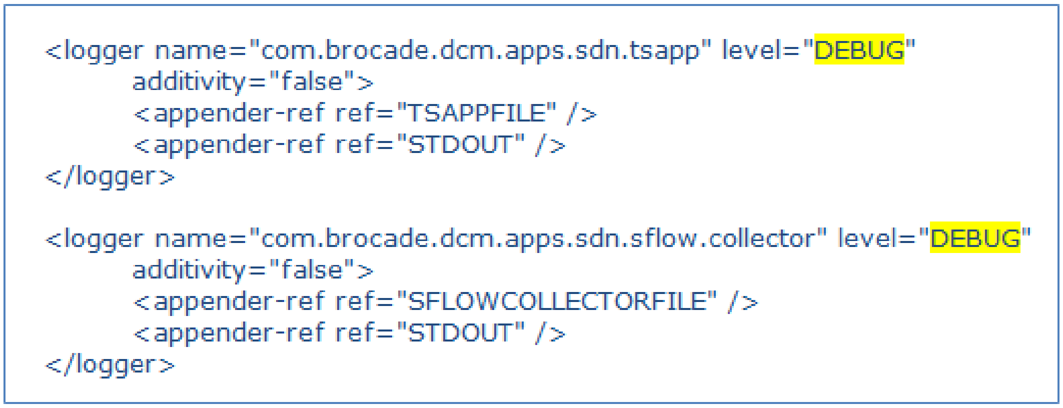
- (Optional) Changing the Logging Level on page 104
- Generating Support Save Data on page 105

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:

- 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

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

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

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

Code	Message
2014	Invalid input parameters-start time is greater than end time
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

Profile Validation

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

Code	Message
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
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}

Code	Message
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
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

Code	Message
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

sFlow Settings

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

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

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

Code	Message
9001	The checksum is not valid. Please provide the valid checksum
9002	Please provide the checksum ID or atleast one match criteria in the flow
9003	Please provide the valid priority. Valid range: 1- 65535
9004	Invalid IP Type. Please provide the valid type of IP Address (ipv4 / ipv6) if you provide the ip address
9005	Source Port and Destination port should be empty, if the IP Protocol is None or empty
9006	Destination port is invalid
9007	Invalid redirection parameters. Ensure to set RedirectActionParameters when redirect action is selected
9008	SDN Controller settings in Brocade Flow Optimizer are not configured or controller is not reachable.
9009	No Open flow enabled ports in the device {0}.

Code	Message
9010	The device {0} is not discovered in controller
9011	Invalid MAC address in set destination field
9012	Invalid VLAN ID in set destination field
9013	Invalid meter parameters. Ensure to set MeterActionParameters when METER action is selected
9014	The port {0} is not present in device {1}
9015	Invalid mirror parameters. Ensure to set MirrorActionParameters when MIRROR action is selected
9016	The ingress port and mirror port should belong to same device.
9017	The ingress port and mirror port should not be same.
9018	You cannot select multiple ingress port in redirect action if you choose to set MAC or VLAN ID
9019	Failed to create a user defined flow on the Device. Please verify the device logs for more information
9020	Failed to delete a flow. Invalid Flow ID {0}
9021	Invalid Priority for user defined flow. Valid Priority ranges Above Learned and Programmed: 36001 - 65535. Below Learned and Programmed: 1001 - 32000
9022	The Priority {0} is already used by other flow. Please provide a new priority or delete existing flow to freeup the priority