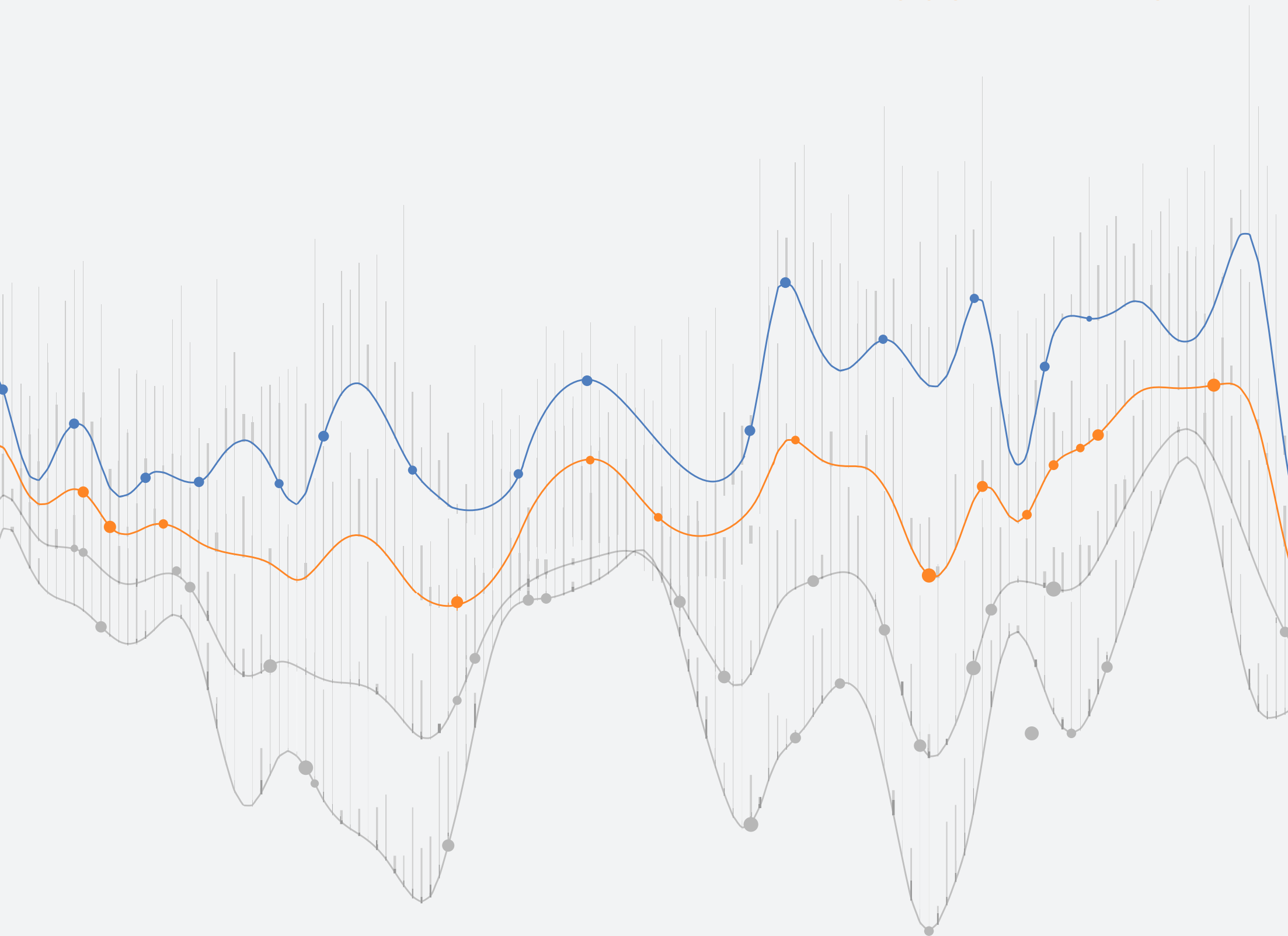




# Noction Flow Analyzer

DOCUMENTATION



# Table of Contents

---

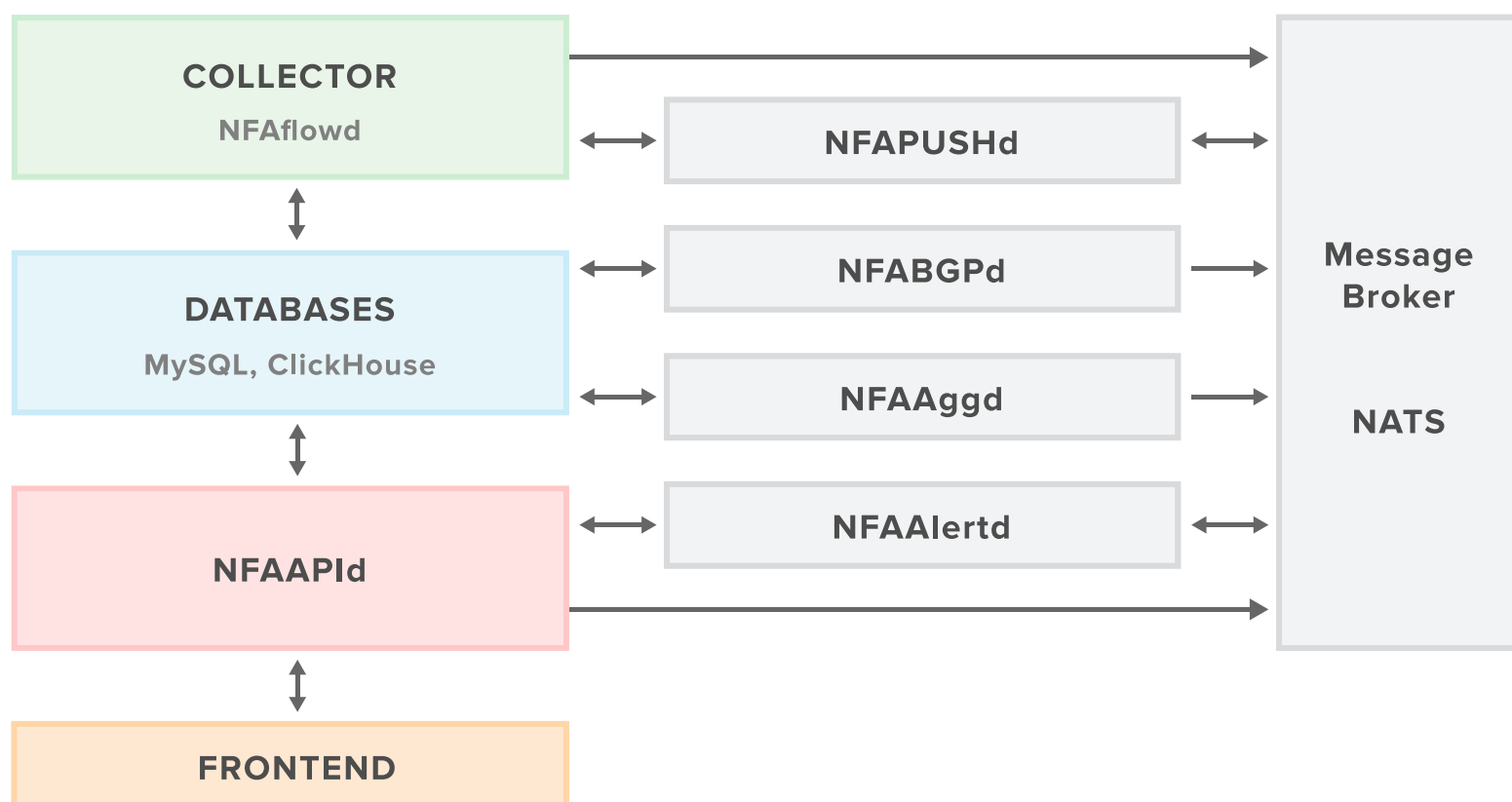
- 1. NFA Overview.....3**
  - 1.1 NFA Components.....3
  - 1.2 Collector.....4
  - 1.3 Databases.....5
- 2. NFA Functionality.....6**
  - 2.1 Frontend.....6
    - 2.1.1 Dashboards.....8
    - 2.1.2 Widgets.....11
  - 2.2 Data Explorer.....13
    - 2.2.1 Group & Order.....14
    - 2.2.2 Filters.....15
    - 2.2.3 Filtering by Devices.....17
    - 2.2.4 Time Intervals.....17
    - 2.2.5 Percentile reporting.....18
  - 2.3 BGP Data.....18
    - 2.3.1 BGP Report.....19
    - 2.3.2 BGP Sankey Diagram.....20
  - 2.4 SNMP Data.....21
  - 2.5 Alerts.....23
    - 2.5.1 Creating Alerts.....23
    - 2.5.2 My Alerts.....25
    - 2.5.3 Active Alerts.....25
    - 2.5.4 History of Alerts.....25
- 3. Management.....26**
  - 3.1 Inventory.....26
    - 3.1.1 Adding Devices.....26
    - 3.1.2 Managing Devices.....29
    - 3.1.3 Deleting Devices.....30
  - 3.2 Configuration Settings.....30
  - 3.3 Custom Groups.....30
  - 3.4 Dictionaries.....33
    - 3.4.1 MAC Addresses.....33
    - 3.4.2 PTR Records.....33
  - 3.5 System Notifications.....33
    - 3.5.1 System Notifications Overview.....33
    - 3.5.2 System Notification Channels Configuration.....34
    - 3.5.3 System Notification Subscriptions.....35
    - 3.5.4 Notification Text Details.....35
  - 3.6 User Management and User Directories.....36
    - 3.6.1 User Management.....36
    - 3.6.2 LDAP User Directories.....36
    - 3.6.3 TACACS+ user directories.....38
  - 3.7 SSL/TLS Certificates.....40
  - 3.8 Personalization.....40
  - 3.9 License Status.....41
  - 3.10 API Documentation.....41
  - 3.11 NFA Version.....42
  - 3.12 NFA Changlog.....42
  - 3.13 Billing Info.....42
- 4. User Profile, Requirements, Support.....43**
  - 4.1 User Profile.....43
  - 4.2 System Requirements.....45
  - 4.3 Support.....45
- 5. Flow export configuration on network devices.....45**

# 1. NFA Overview

Noction Flow Analyzer (NFA) is a web-based network traffic analysis, monitoring and alerting tool. The product enables engineers to optimize their networks and applications performance, control bandwidth utilization, do the proper network capacity planning, perform detailed BGP peering analysis, improve security, and minimize network incidents response time.

## 1.1 NFA Components

Noction Flow Analyzer contains a few fundamental components, which working together implement the main function of NFA - offer timely traffic flows information that is easy to interpret and analyze.



**Collector** (NFAflowd) receives, analyzes, and processes all traffic transiting a network.

**Databases:** NFA uses two databases: MySQL (configuration) and ClickHouse (Data Mart), that act relating to the central repository which stores processing results.

**NFAAPId** represents a set of secure web services that collect data from Databases. A valid NFA user-id is required to access most of the API services. Access NFA’s frontend to manage users or configure external User Directories. NFA API uses an authentication mechanism based on authentication tokens. The token is passed as a query parameter for all API requests that require authentication.

**NFABGPD** stores and keeps all routes and adds AS Path to traffic flow.

**NFApushd** is used to send notifications and alerts to the end-users.

**NFAaggd** periodically aggregates flow data that is stored in the database and flushes data according to the configuration parameters

**NFAalertd** is used to detect and generate alerts based on the alert settings set by the end-user.

**Msg. Broker** is used for communication between the NFA components.

**Frontend** represents a complex browser application that interacts with NFAAPId. It offers a comprehensive set of reports, graphs and flows information that can reflect the current and historical state of a network.

## 1.2 Collector

The collector is one of NFA's most important components. It receives, analyzes, and processes all traffic transiting the network and transfers data in a compatible mode to NFA Databases – MySQL and ClickHouse. It processes the most common types of Flow: NetFlow, sFlow, J-Flow, IPFIX, NetStream.

sFlow (6343 port) is a protocol designed for monitoring network, wireless and host devices. Developed by the sFlow.org Consortium, this protocol is supported by a wide range of network devices, as well as routing software and network solutions. sFlow, short for "sampled flow", is an industry-standard for packet export at Layer 2 of the OSI model. It provides the means for exporting truncated packets, together with interface counters. It's a packet sampling for an N number of packets with all required statistical information and expedited to the destination collector. The information details taken from the packet are the headers from Layer 3 and 4 and some information about the upper layers' data only. For example, if the HTTP protocol is present, sFlow will guarantee data confidentiality since it will not extract the information from the packet and will not collect all network sessions.

NetFlow (2055 port) is an IP network statistics protocol developed by Cisco Systems, Inc. that offers the ability to collect IP session network traffic as it enters or exits an interface. By analyzing the data that is provided by NetFlow a network administrator can determine things such as the source and destination of traffic, class of service, and the cause of congestion. Juniper routers offer a similar feature called J-Flow which in its essence is the same Cisco NetFlow protocol.

Flow statistics are captured and stored in DB which NFA's graphical interface subsequently offers to users as dashboards, charts, and reports with filtering, grouping, and aggregation functions.

Network devices should be first configured to forward Flow statistics to NFA in order for it to get the initial data to operate on. NFA listens to Flow stats on the default protocol ports. Flow ports can be changed from the Configuration Settings section of NFA's Front End.

**Note:** Set the frequency of Flow exports on network devices as frequently as possible. For best results export intervals should be set to 1 min or even less.

---

## 1.3 Databases

NFA processes huge volumes of data and uses two databases to store all the related information: MySQL and ClickHouse. The accumulated information is used by other NFA components to provide a graphical view of flow parameters.

MySQL is the most popular Open Source SQL database management system, developed, distributed, and supported by Oracle Corporation. It plays the role of NFA's system data depository which possesses configuration, dashboard, device, and user information.

ClickHouse is a column-oriented database management system (DBMS) for the online analytical processing of queries (OLAP).

### **ClickHouse benefits:**

- Extremely Fast scans that can be used for real-time queries.
- Real-time data ingestion
- Parallel processing for a single query
- Hardware efficient
- Scales well both vertically and horizontally

### **The most important ClickHouse tables are:**

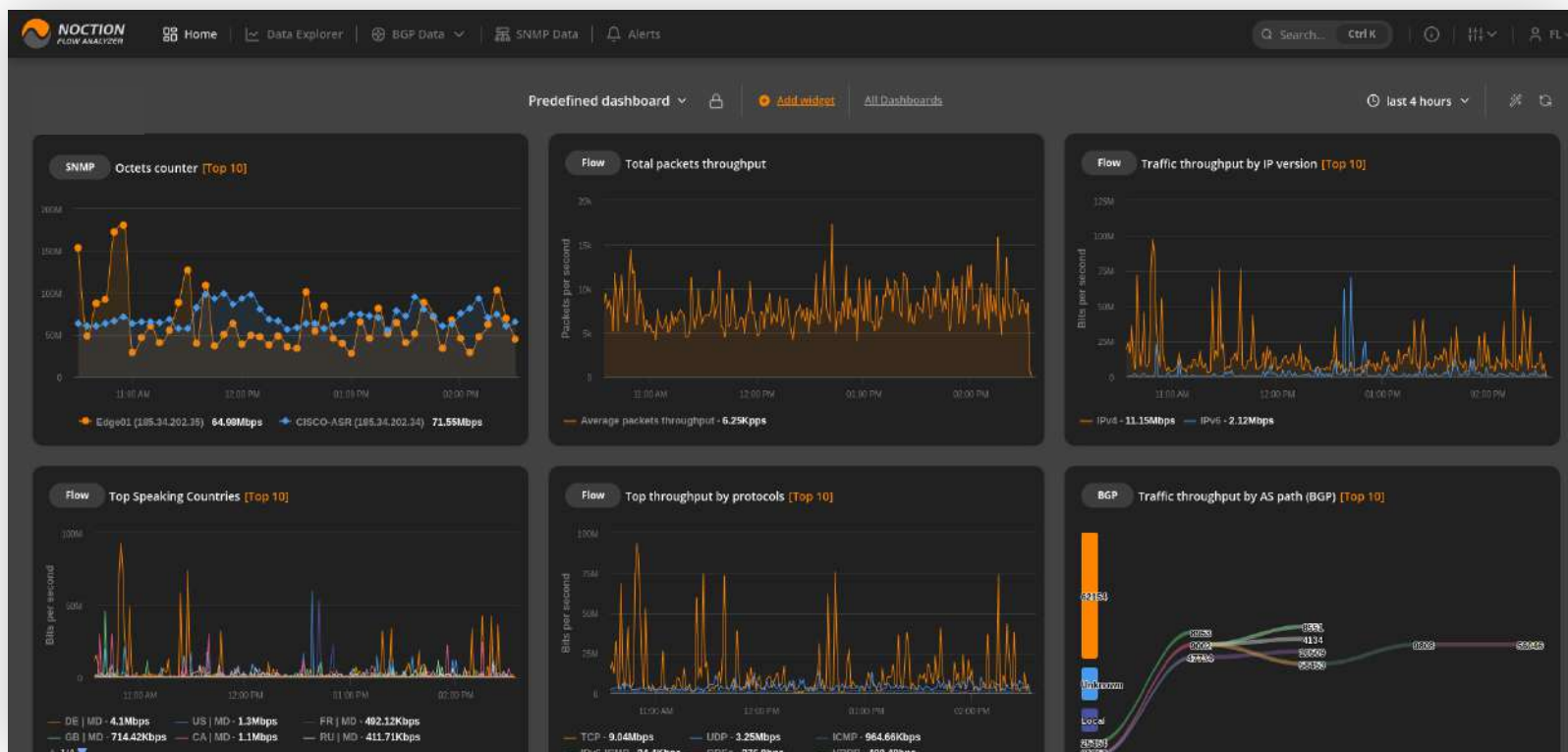
- BGP
- Database\_version
- Flows1
- Flows2
- Raw
- Template\_flows

Flows Tables comprise the meaningful flow data.

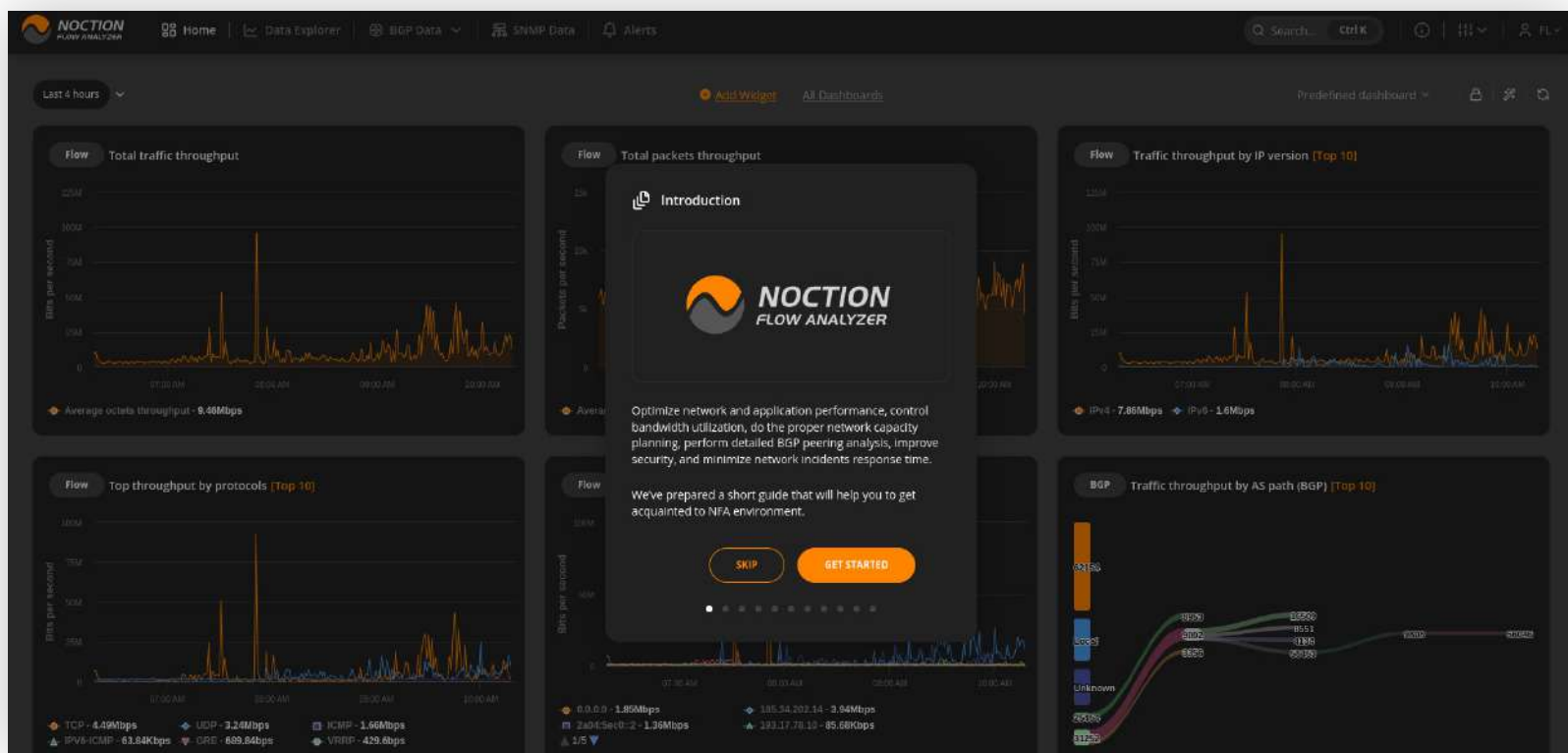
## 2. NFA Functionality

### 2.1 Frontend

NFA main page is designed to display a dashboard of choice and offer facilities to access all application features via its main menu, navigation buttons, and links. Use Global Search (Ctrl K) to effortlessly steer the application using keyboard shortcuts.

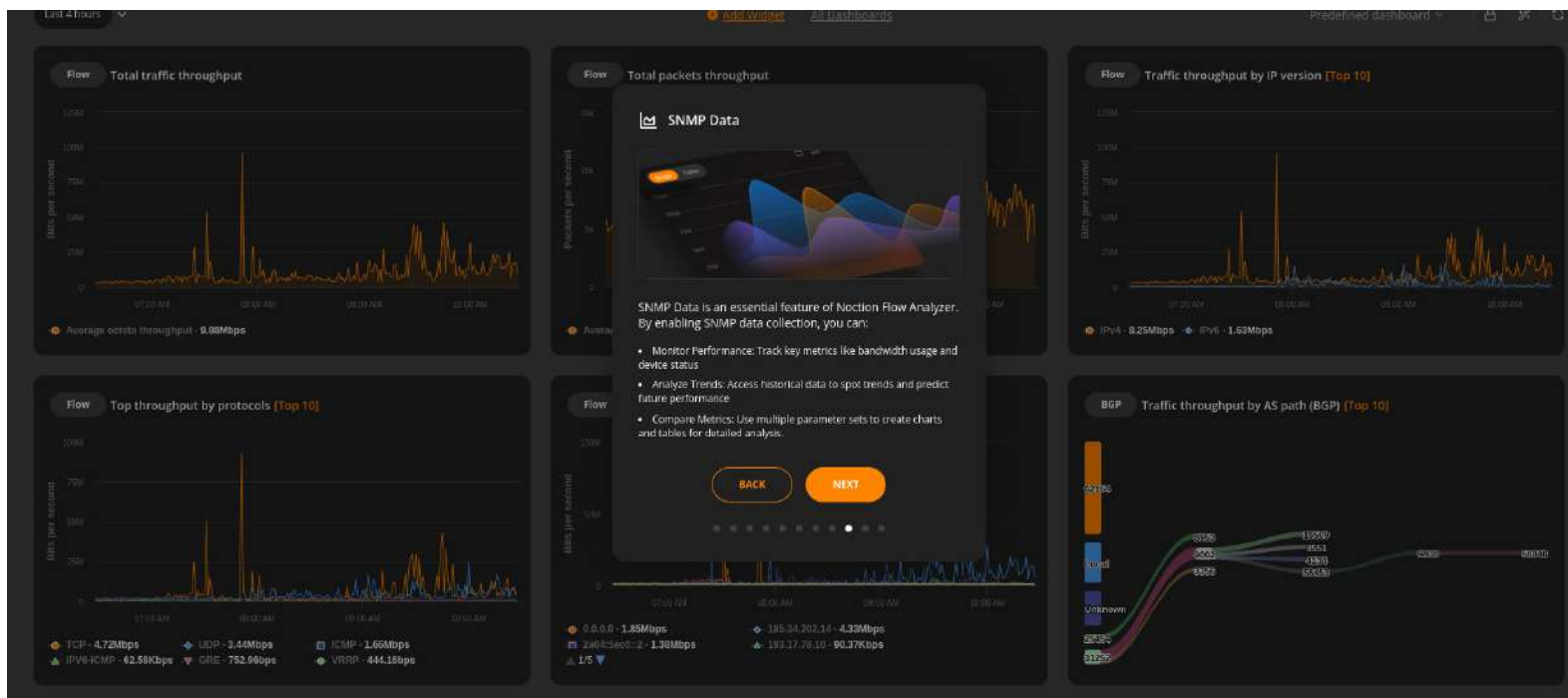


When installing NFA for the first time, a Welcome Wizard pops up on the screen. It showcases and guides you through the system, displaying the list of available NFA features and how they work. This makes the first-time user understand all the product capabilities & configuration procedures a lot easier and faster.

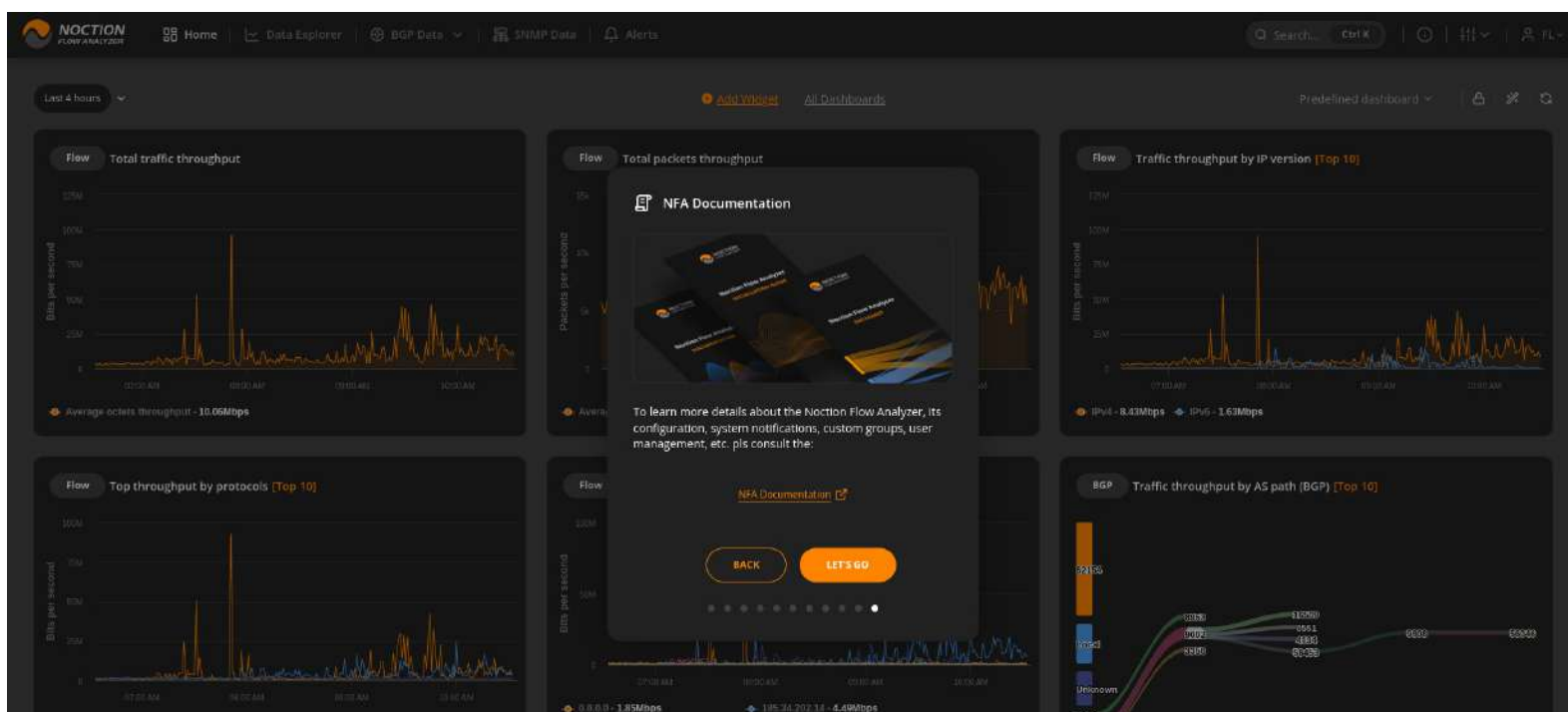


If at any time you decide to go through the wizard steps again, you can do so by navigating to your **Username > Profile > General** and restarting the wizard.

When you click on “Get Started,” you’ll be guided through key information about NFA. The first step introduces you to Licensing, where you can view your License status, ID, and even change the license. Next, you’ll have the option to customize your theme, choosing between light, dark, or auto modes. As you continue, you’ll explore the main resources and functionalities of NFA, including Adding/Editing Devices, NFA Dashboards, Data Explorer, Alerts, BGP Data, SNMP Data, and SSL/TLS Certificates. An example you can see in the image below.

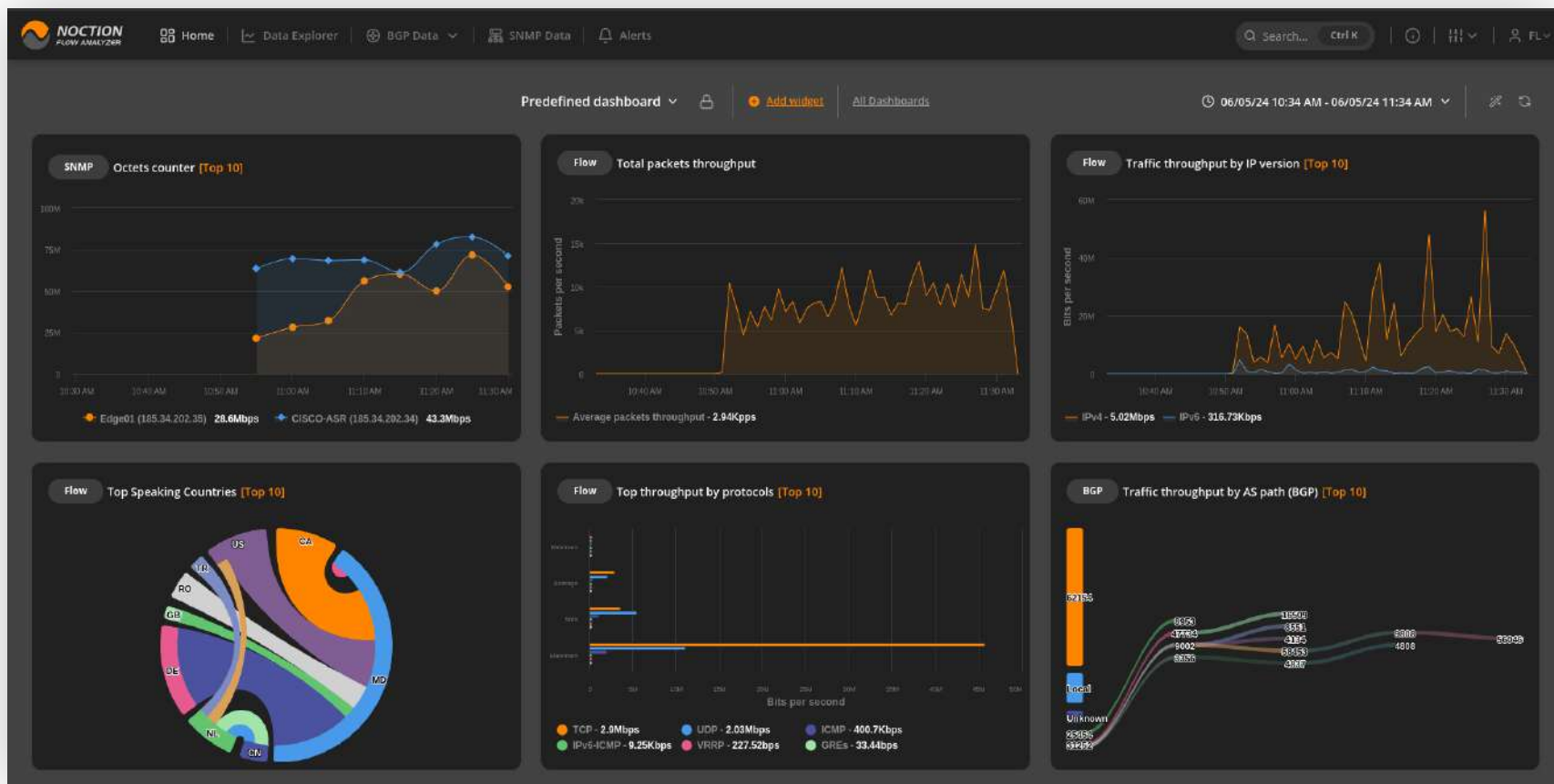


Additionally, the Welcome Wizard provides easy access to the NFA Documentation, ensuring you have all the resources you need at your fingertips.

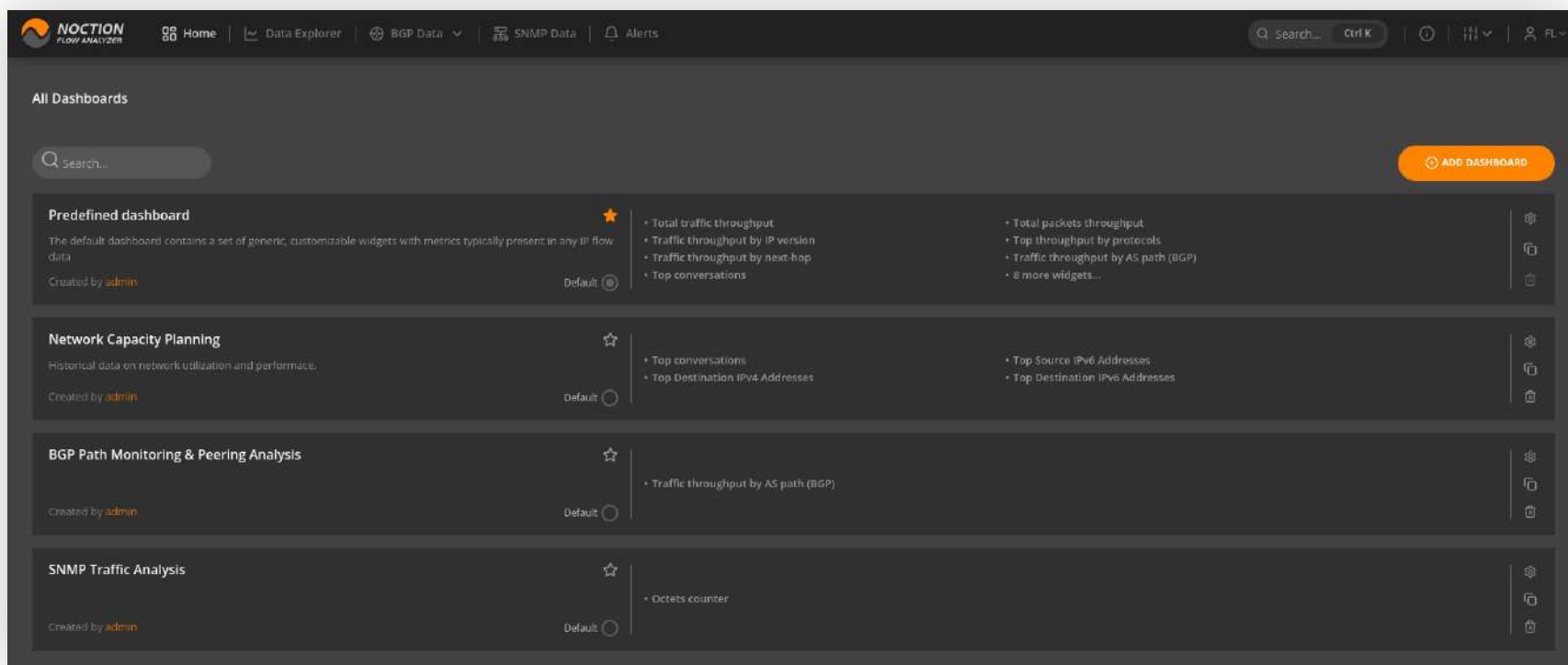


## 2.1.1 Dashboards

NFA dashboards are the specific sets of flexible and interactive visualizations, designed for quick analysis of the network traffic data and informational awareness. Dashboards consist of widgets – containers with graphical representations of specific data, which can be added, edited, positioned, deleted or modified as you like.



NFA allows users to set up multiple dashboards. To see a list of existing dashboards, click the **All Dashboards** link in the top menu.





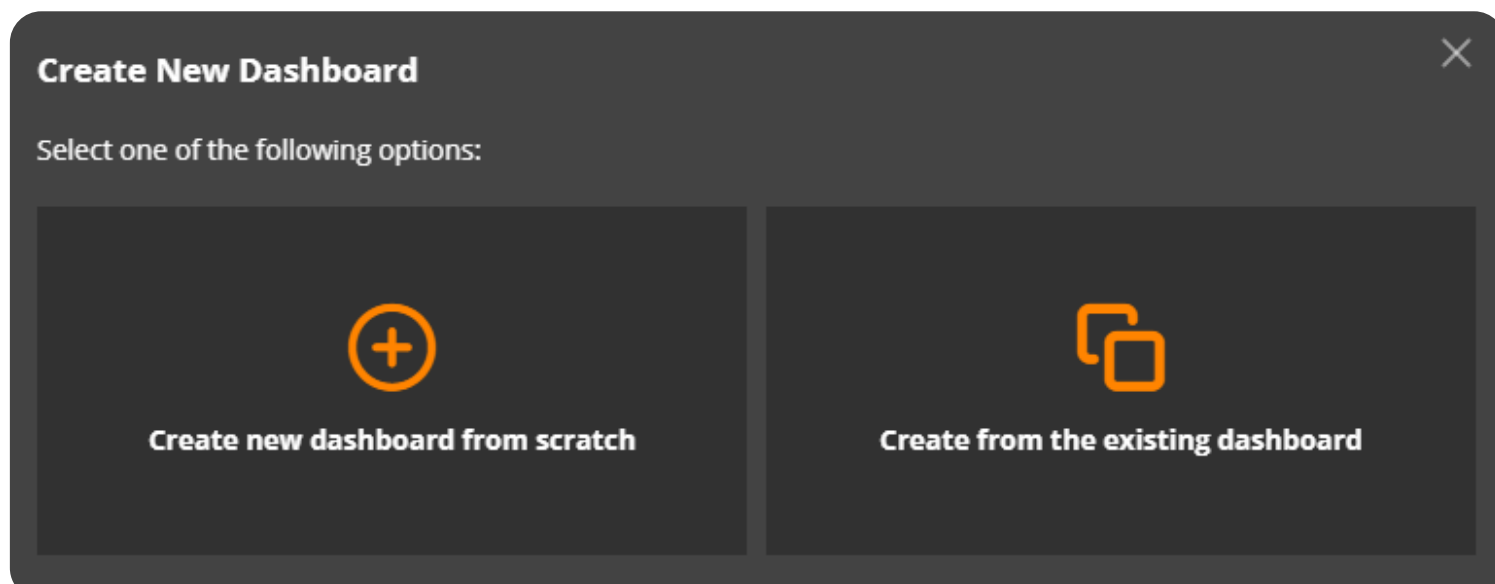
Dashboards are grouped for easy access into recent, favorite and all. For each dashboard, the directory displays the following information:

- **Name:** The name of the dashboard
- **Description:** Dashboard user-defined description
- **Favorite:** a state marked by a star icon
- **Created by:** The user who created the dashboard
- **List of widgets:** widget names used in the dashboard
- **Default status:** the default dashboard the user lands on when logging into NFA

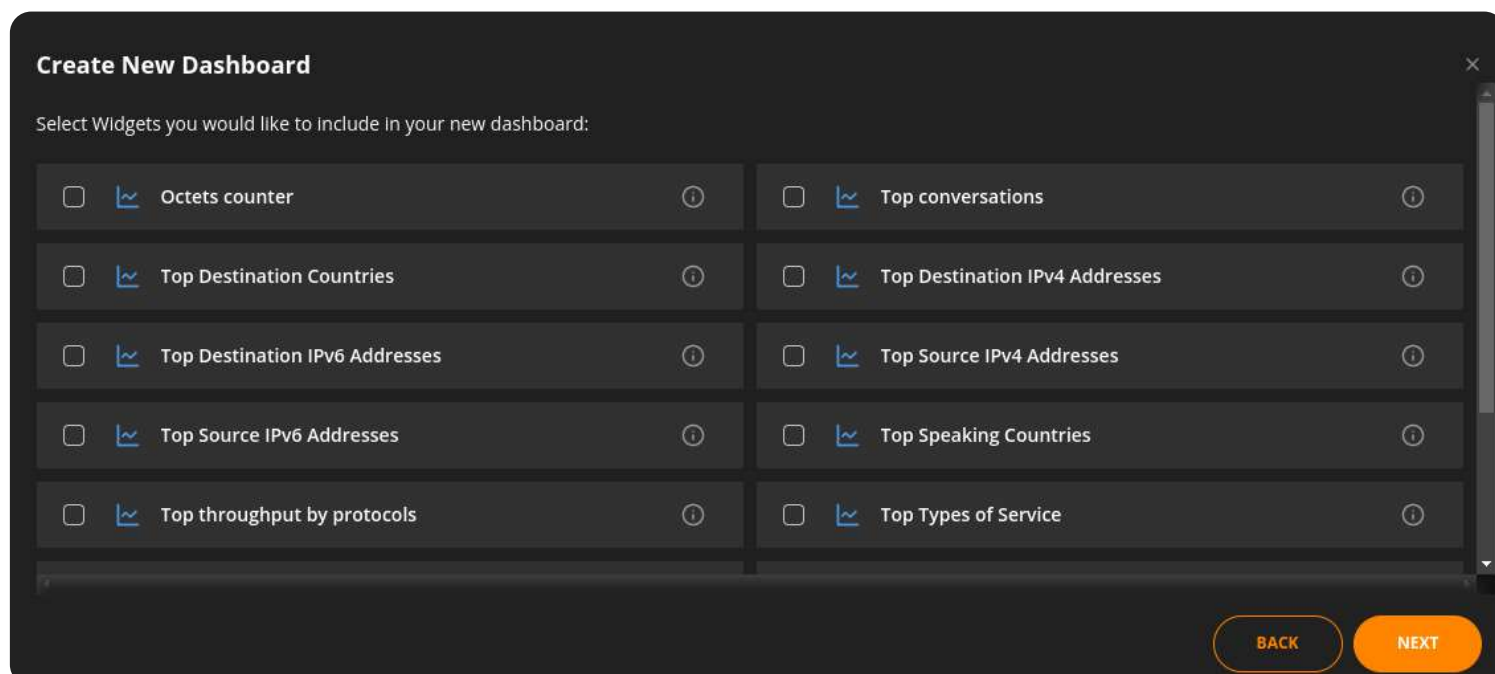
### Creating a new dashboard

You can easily create a new dashboard in NFA from the All Dashboards directory.

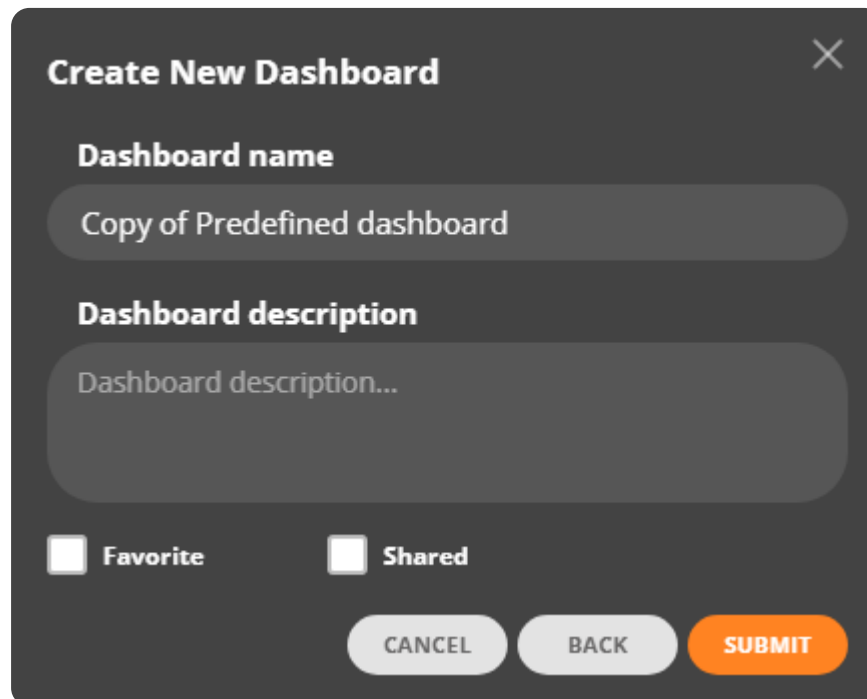
Click the “**ADD DASHBOARD**” button. A pop-up will appear. Choose if you’d like to create a dashboard from scratch or build one based on an existing dashboard.



Select the widgets you’d like to add to your dashboard.



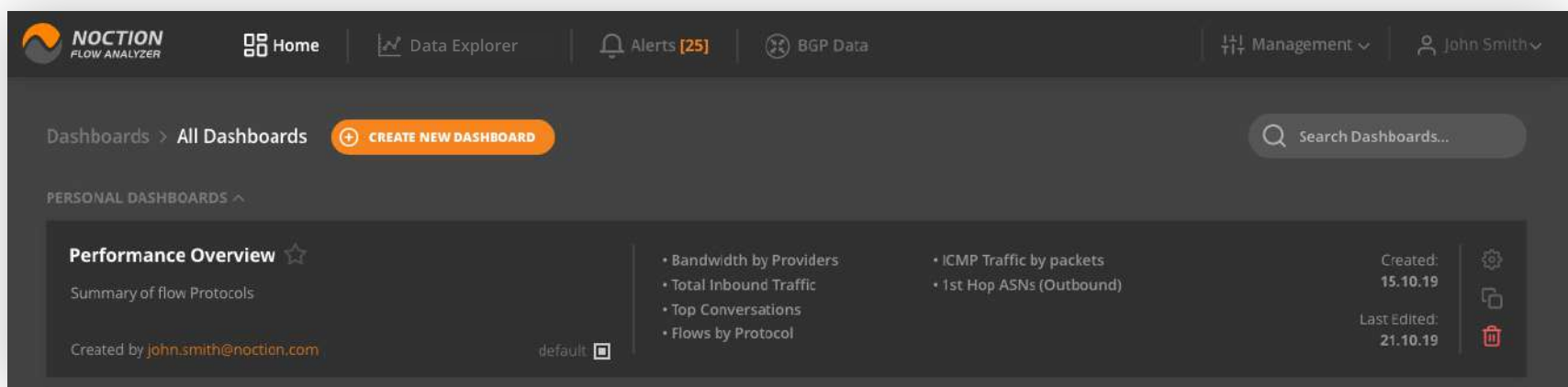
Provide a meaningful name and description for your dashboard. Mark if you'd prefer it to be a **"Shared"** (all NFA users will have access to dashboard) and/or **"Favorite"** dashboard. Press **"SUBMIT"** to continue.



The form is titled "Create New Dashboard" and contains the following fields and options:

- Dashboard name:** A text input field containing "Copy of Predefined dashboard".
- Dashboard description:** A larger text input field containing "Dashboard description...".
- Favorite:** A checkbox that is currently unchecked.
- Shared:** A checkbox that is currently unchecked.
- Buttons:** Three buttons at the bottom: "CANCEL" (grey), "BACK" (grey), and "SUBMIT" (orange).

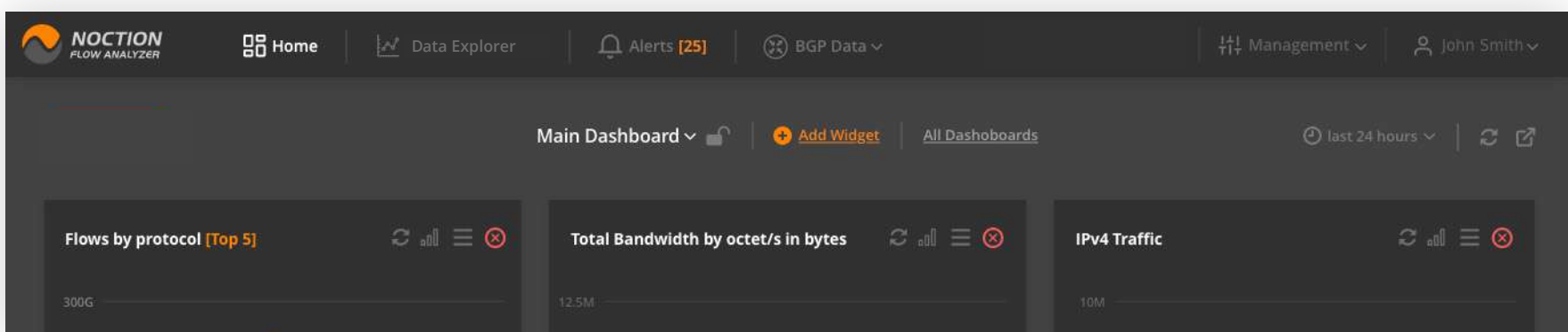
Alternatively, you can create a new dashboard by cloning an existing one in the All Dashboards directory.



The clone dashboard will be automatically created along with widgets from the original dashboard and added to the directory. Edit the newly created dashboard to change its name and description.

### Managing Dashboards

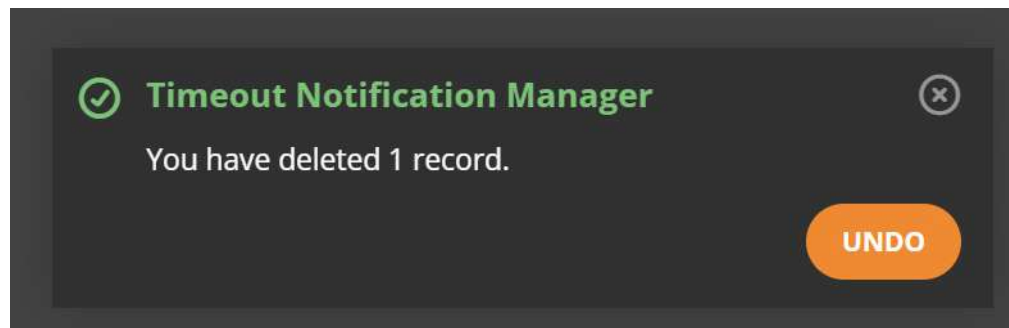
Access any of the dashboards you've created or had admin rights to. Click the padlock icon in the top menu to add, edit and delete widgets or customize the dashboard's layout.



## Deleting a Dashboard

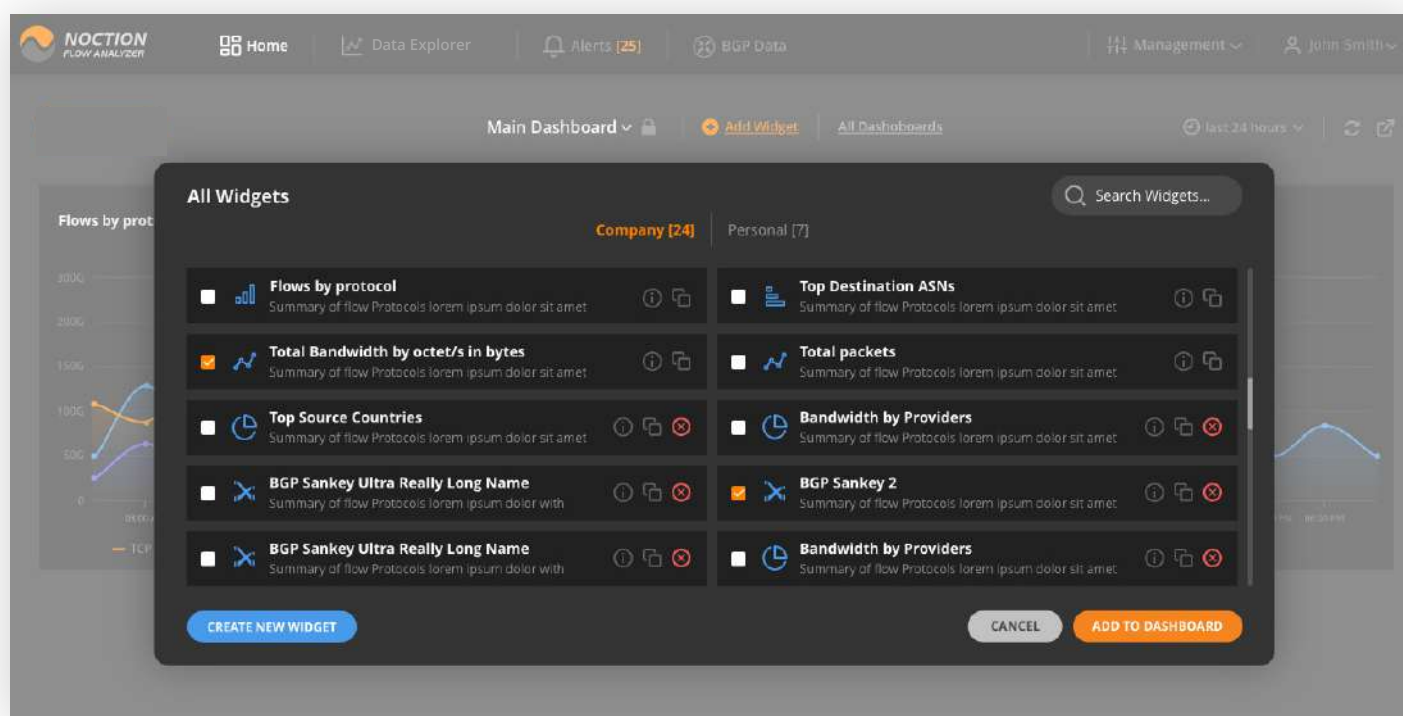
Click the “**Delete**” icon on the dashboard you’d like to get rid of in the **All Dashboards** directory. You can only delete a dashboard if you created it, or if you’ve been granted the corresponding admin rights.

Timeout allows you to undo the unintentional deletion action for dashboards, preventing the accidental deletion of critical information.

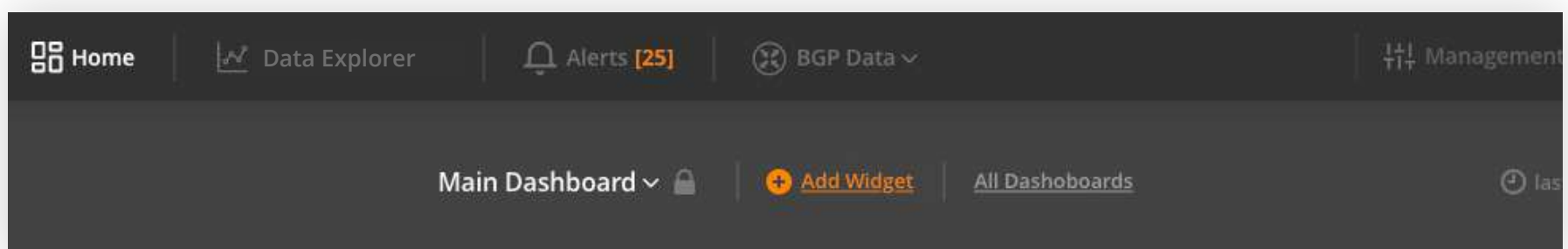


## 2.1.2 Widgets

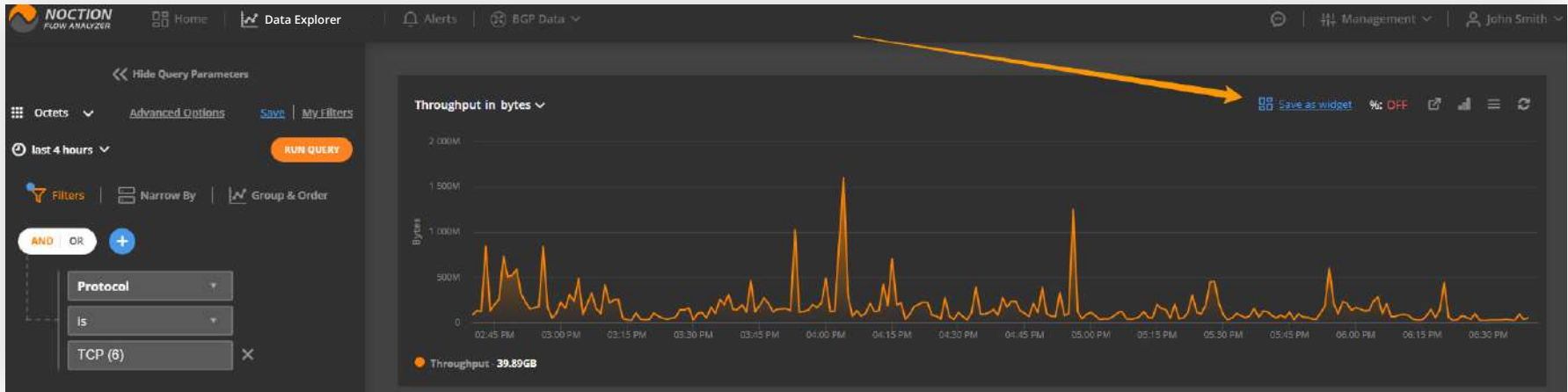
All network traffic information in NFA is graphically represented by widgets, which are the main dashboard elements. Widgets encompass a particular query focusing on the desired network feature. A library of widgets is maintained by NFA and allows users to reuse them across all dashboards.



Use the Add Widget function available on each dashboard to see the library of existing widgets and place the desired ones on a dashboard.

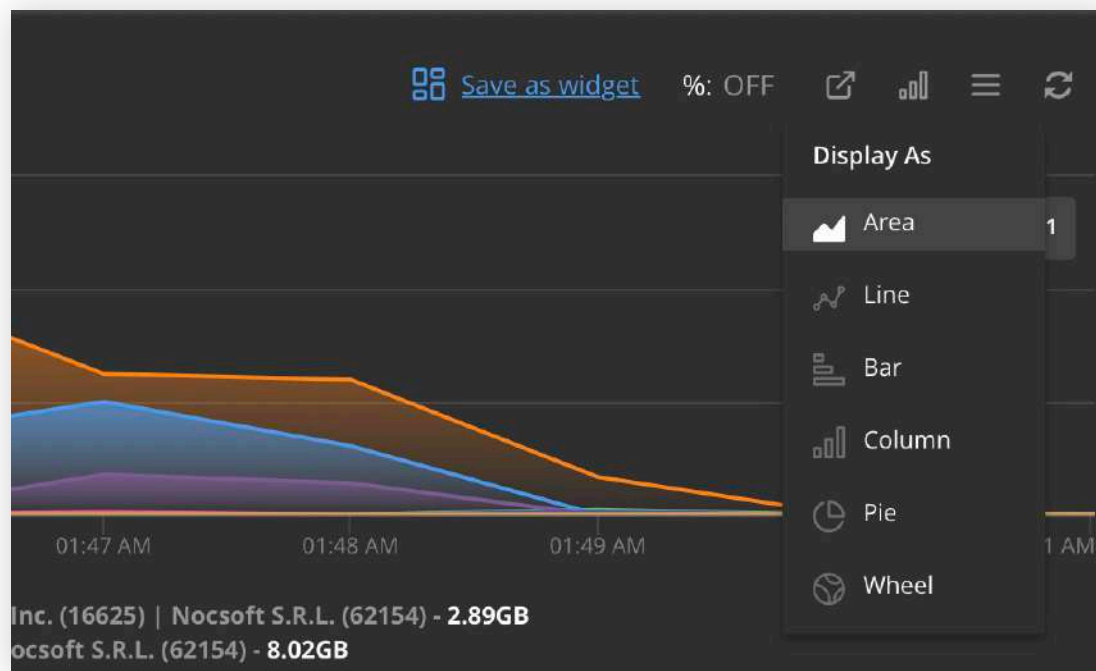


You can easily create a new widget from scratch by proceeding to **Data Explorer** in the top menu, selecting the filtering and grouping options and subsequently saving the Data Explorer view as a new widget to the desired dashboard.

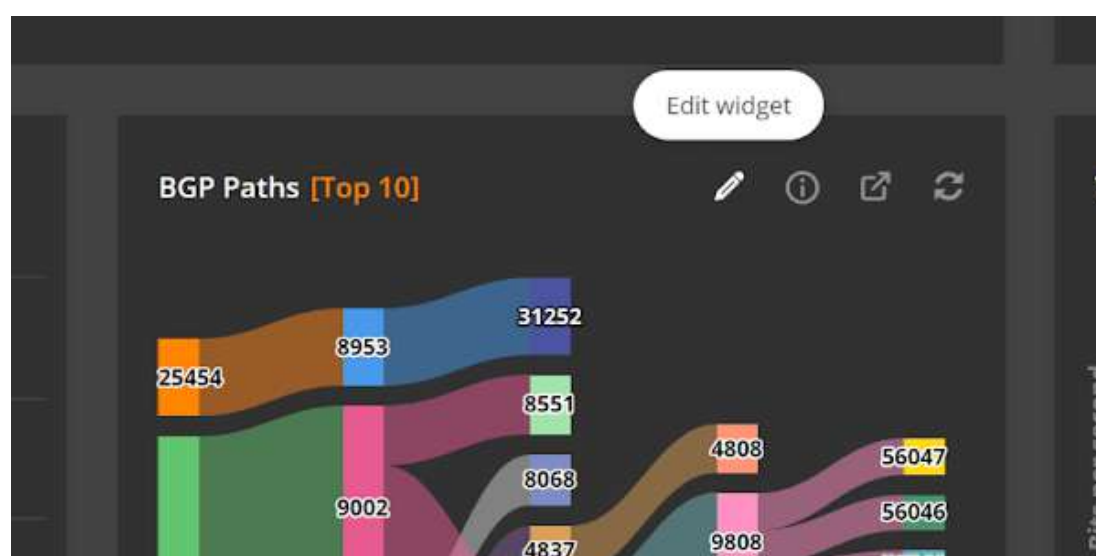


Alternatively, you can create a new widget by duplicating an existing one. Click on the existing widget name to open it in **Data Explorer**. Make desired modifications and save it as a new widget.

Feel free to change the widgets graph settings, appearance as well as the legend position by clicking the appropriate buttons in the top right corner of the Data Explorer graph or the actual widget.



To edit an existing widget, click the corresponding icon next to its name either in the widget library or on a dashboard. Please note that predefined widgets can not be edited.



## 2.2 Data Explorer

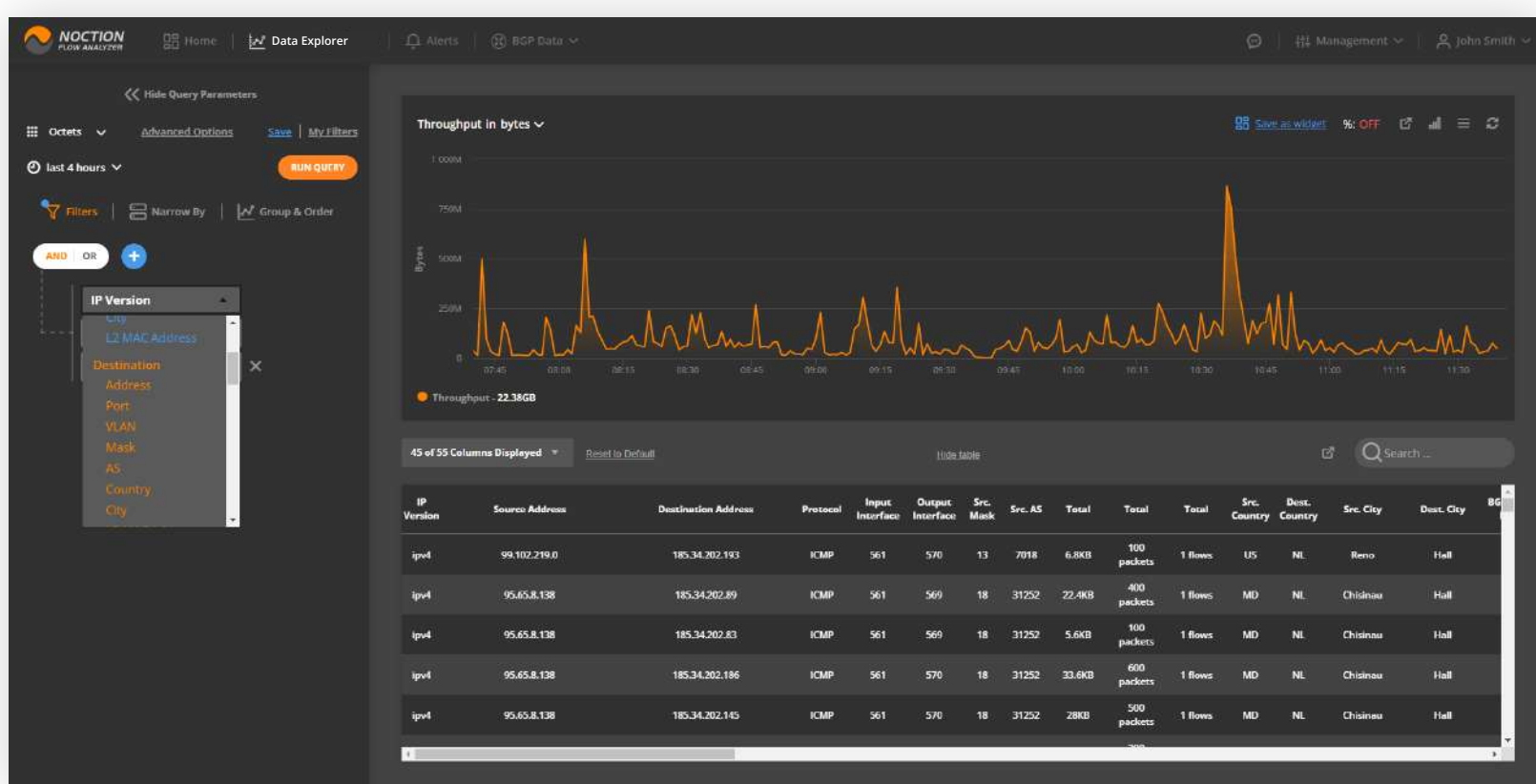
Data Explorer provides detailed network traffic stats in both chart (when possible) and report forms. “**Group & Order**”, “**Filters**” and “**Narrow by**” functions are available to focus or broaden attention to the desired aspects of network traffic.

Data Explorer can be accessed either from the Main Menu or by clicking on any widget’s header on dashboards. Any grouping and filtering criteria previously setup in widgets will auto-populate in Data Explorer.

Data Explorer takes the ensuing statistics from the DB table Flows which includes but is not limited by the following:

- Time
- Source and Destination Address
- Source and Destination Port
- Source and Destination VLAN
- Source and Destination Mask
- Source and Destination AS Number
- Source and Destination AS Path
- Source and Destination AS Path
- Source and Destination Country
- Source and Destination City
- Source and Destination L2 MAC Address
- MPLS Top Label to Top Label 9
- MPLS Top Label Type
- MPLS Top Label IPv4 Address
- MPLS Top Label IPv6 Address
- MPLS Top Label Prefix Length
- MPLS VPN Route Distinguisher
- MPLS Top Label TTL
- MPLS Label Stack Length
- MPLS Label Stack Depth
- MPLS Top Label Exp
- L3 IP TTL
- L3 IP min TTL
- L3 IP max TTL
- L3 IP Total Length
- L3 IP min Total Length
- L3 IP max Total Length
- BGP Community
- TOS - Type of Service
- Protocol
- Input Interface
- Output Interface
- Next Hop Address
- Pseudowire ID
- Pseudowire Type
- Pseudowire Control Word
- BGP Local Preference
- BGP MED
- L2 Ethernet Type
- Exporter Address
- Exporter ID
- TCP Flag
- Flow Role
- Length
- Exporter AS
- Application Name
- Application Name Custom Group
- Application Name Length
- Source and Destination FQDN address

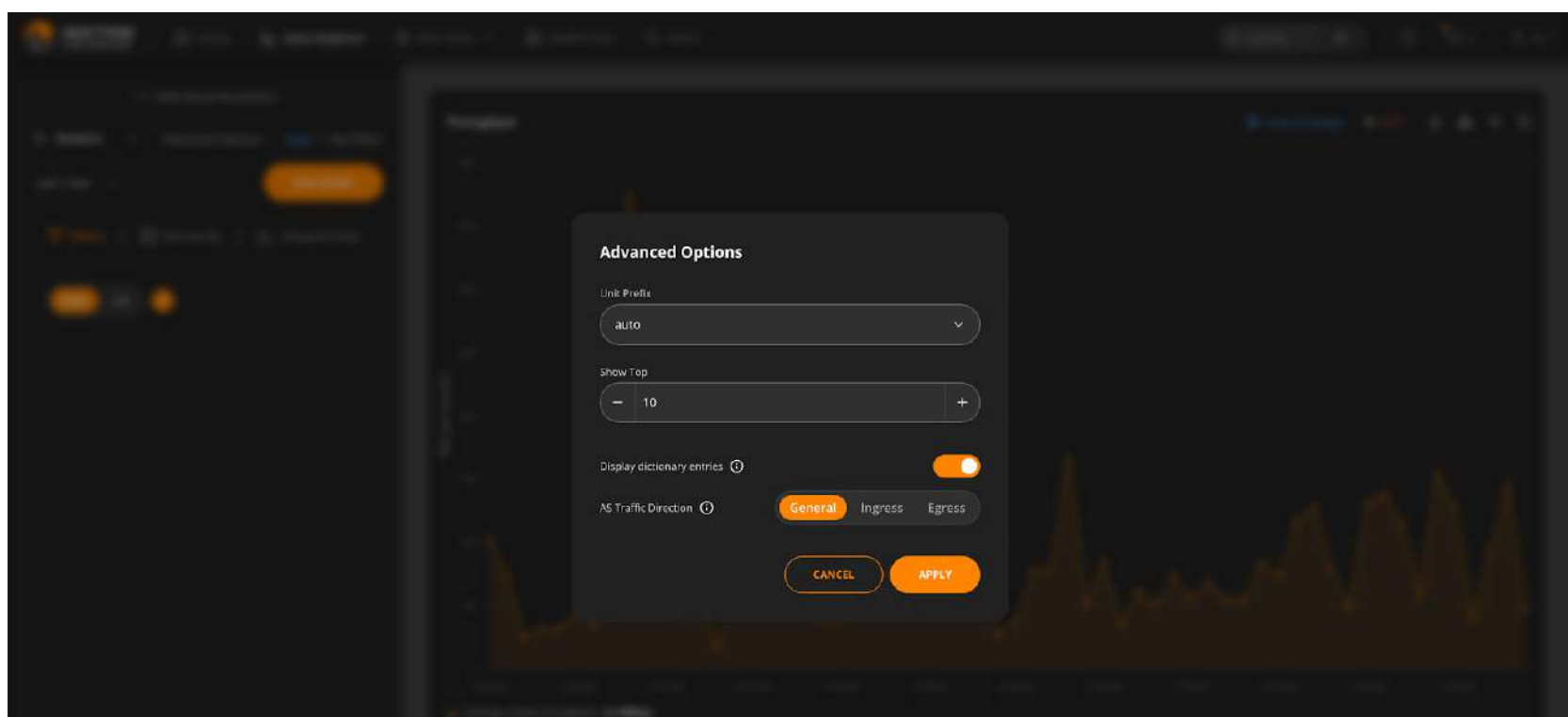
NFA by default uses SUM aggregation functions over Packets and Octets flow metrics.



### Data Explorer functions:

- **Group by** - specifies how to group data.
- **Filters** - specify only the data of interest to include in results
- **Narrow By** - specify from what locations, network devices, and/or interfaces to consider the stats
- **Time horizon** - sets the time interval to explore
- **Packets** depict whether Packets, Octets, bits/s metrics are aggregated and plotted on charts
- **Save | My Filters** allows saving a specific set of selected filters with their corresponding values to “My Filters” library for future use.
- **Run query** - runs the query and retrieves data
- **Save as widget** - prompts for a widget to be added to the library with this exact combo of filters and group by criteria
- **Display as** - chart type icon allows switching between different ways to plot result data

**Note:** The top 10 results are shown by default in Data Explorer and the subsequently created widgets. To change the default settings, go to Advanced options and indicate the desired number of results to be displayed on a graph. You can limit the number of rows to be shown in the table as well. There is also an option to display/hide dictionary entries on graph and legend as well as select the Ingress, Egress, or a combined view of the AS traffic.



Another option allows you to select a specific unit prefix, ensuring that the data displayed in both the graph and table is consistently presented with your chosen unit prefix.

By default, the unit prefix is set to “Auto.” However, you can choose from the following options: auto, kilo, mega, giga, tera, peta, and exa.

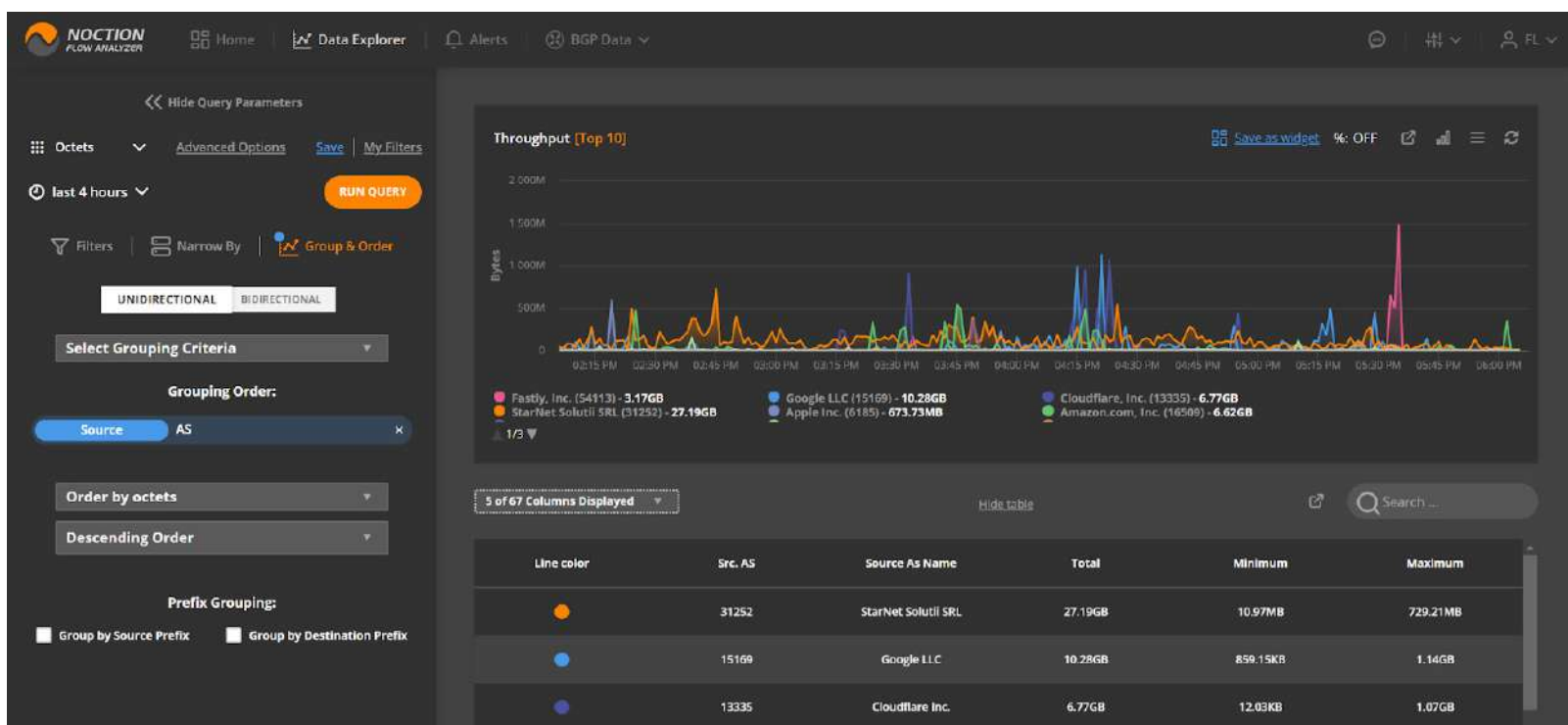
To hide/show specific table columns, click the corresponding “**Hide/Show Columns**” dropdown option.

## 2.2.1 Group & Order

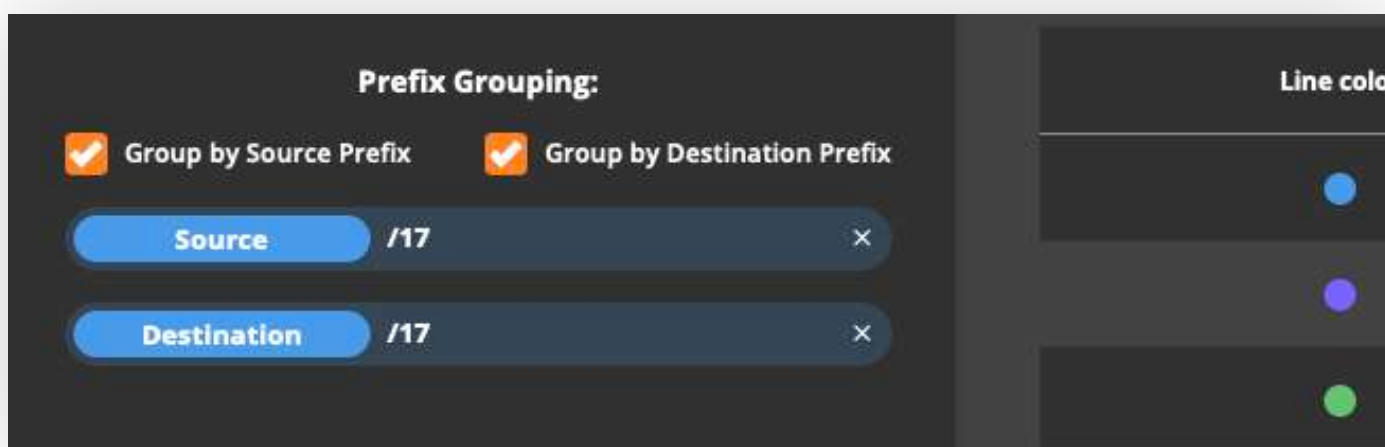
Grouping is one of the essential criteria for analyzing data.

Grouping by source or destination indicates whether the traffic is inbound or outbound. Grouping by the port highlights what amount of traffic the network has for different applications and so on.

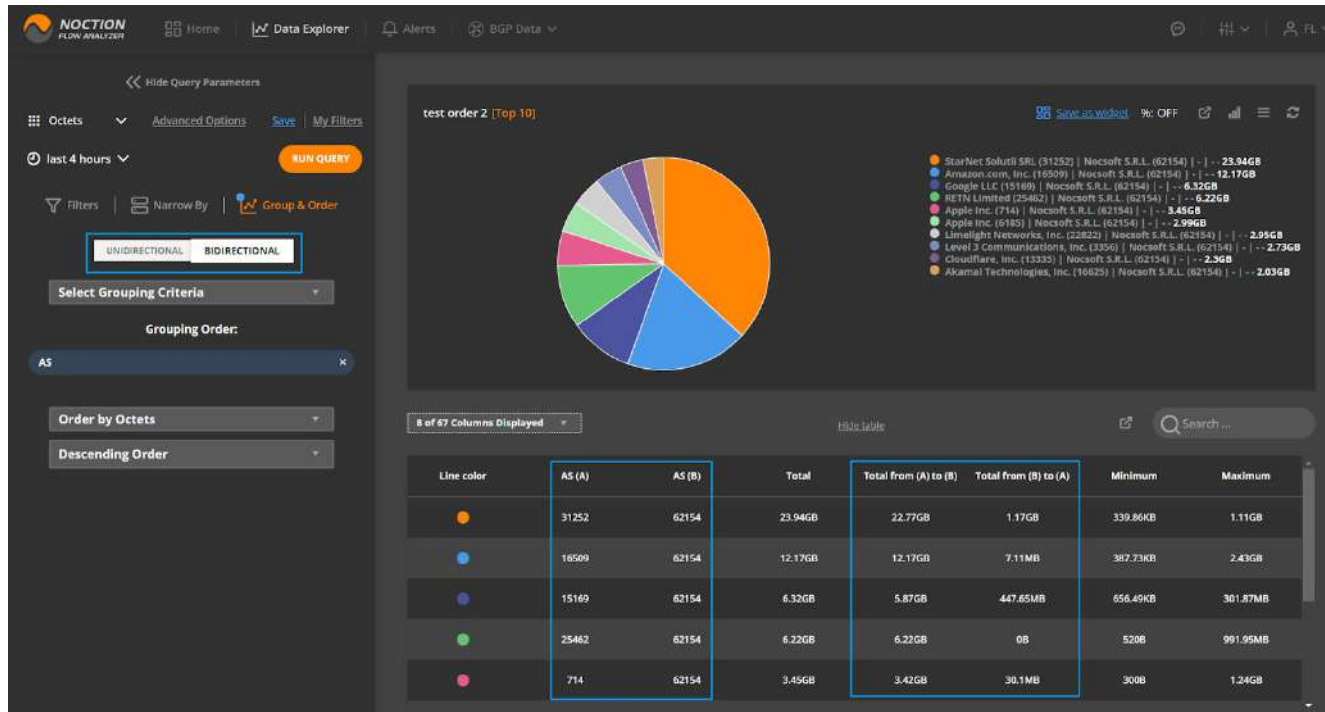
Using the default unidirectional grouping, we can specify one or more Flow attributes to be analyzed. Note that the top results shown in the graph/table can be dependent on a particular traffic direction based on the selected grouping criteria.



To group the results by either all source and/or destination prefixes or by specific prefix sizes, goto **Data Explorer > Group & Order** and introduce the desired prefix grouping parameters.



With the **bidirectional grouping**, traffic between different points (IP addresses, ASes, cities, countries, ports, L2 MAC addresses) will be displayed in a single table/graph with ordering done by the sum of traffic in both directions. When performing queries with bidirectional grouping, the results are shown regardless of the actual source/destination parameter. Instead, they are selected based on the actual amount of traffic, number of flows, etc., passed from one point to another.

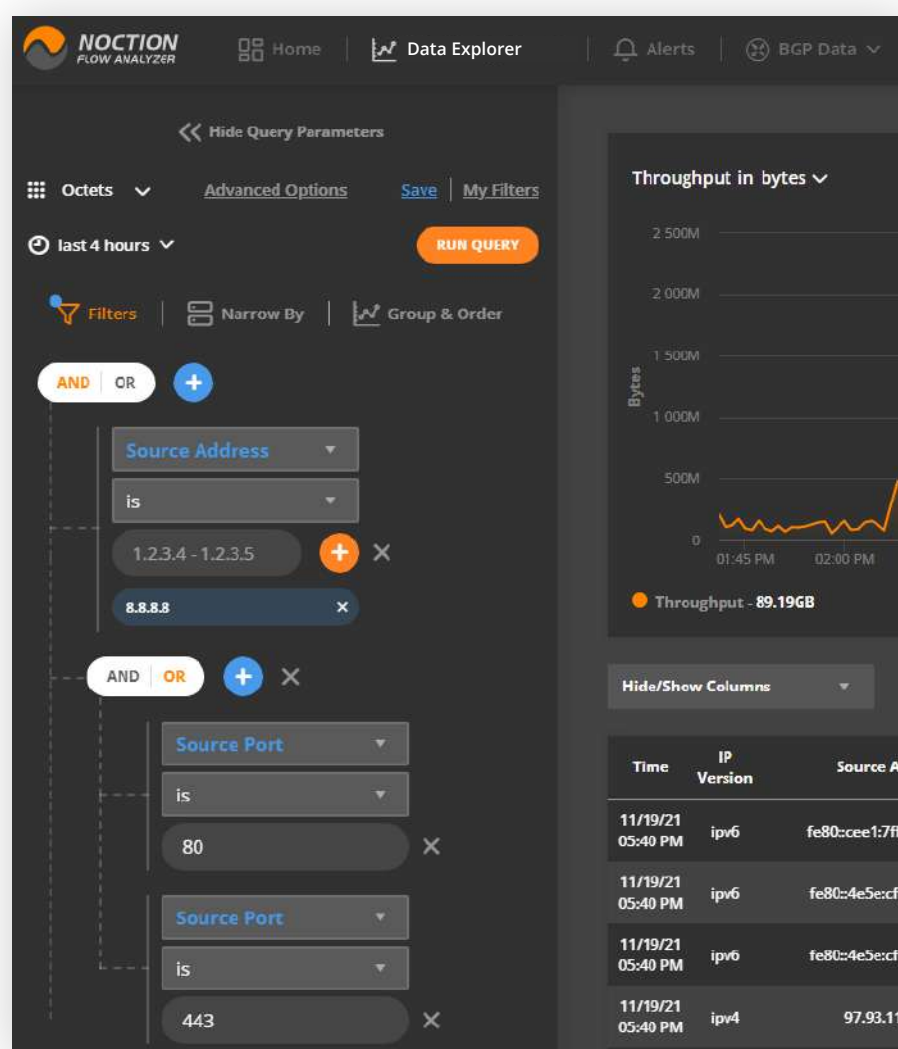


### 2.2.2 Filters

Filters are used to constrain the analyzed data to a particular subset that matches filter criteria. Filters can be applied while working with Dashboards or within Data Explorer. It is a very important feature as it saves time and significantly reduces the workload.

**Note:** NFA applies AND | OR logical operation across conditions or groups of conditions. Thus we can get various sessions like **IP address AND (port = 80 OR port = 443)** when a particular server web traffic is queried.

Preconfigured **Custom Groups** (see section 3.3) can be used as filters. To do so, select a filtering condition, e.g. Source or Destination Address and type in the custom group's name, then run your query.



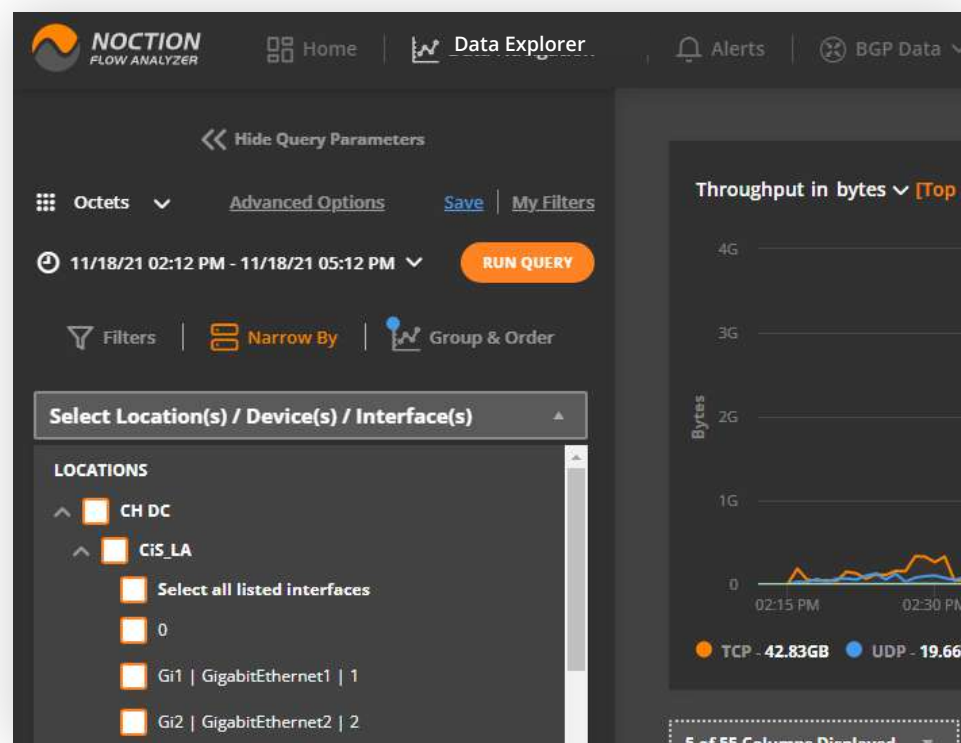


### 2.2.3 Filter by Locations, Devices and Interfaces

NFA users can filter flow data in Data Explorer by devices that have been initially added to the system as well as interfaces. There is an option to select one/multiple devices/interfaces or groups of devices assigned to specific locations (sites).

**Note:** Interface names and descriptions can be identified via NetFlow, IPFIX or NetStream when the flow options template export is set up on the corresponding devices or via SNMP.

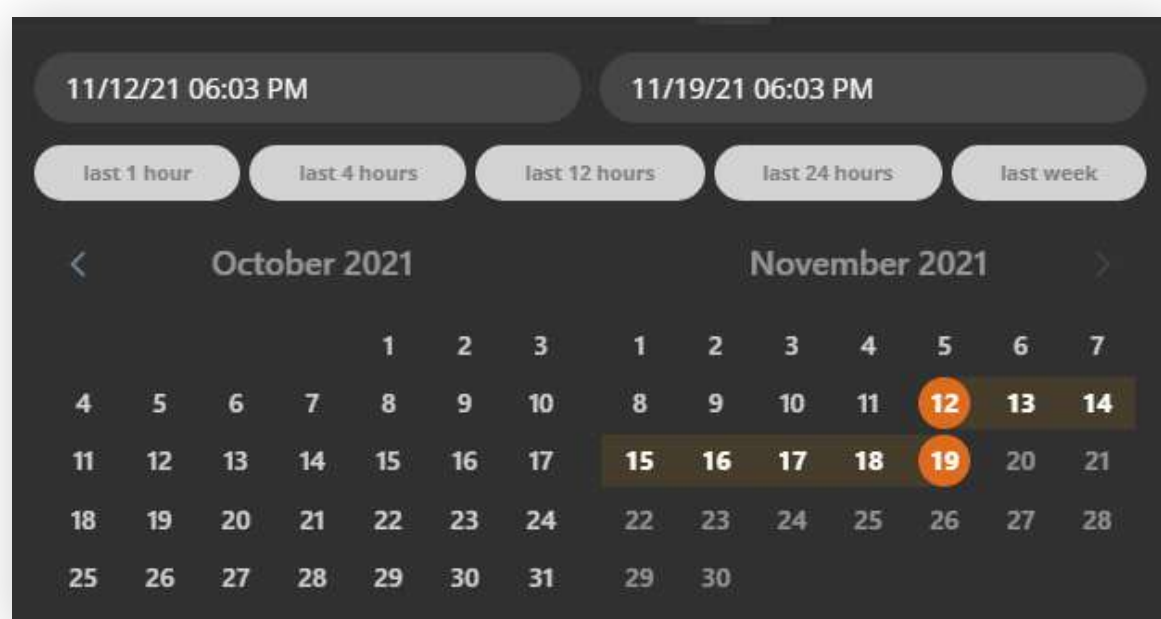
Note that the Flow stats received by NFA and NOT matched to any configured devices will be assigned to a default Not Named device.



Flow sources are matched to configured devices by Exporter IP only or Exporter IP and Exporter ID (if such has been provided).

### 2.2.4 Time Intervals

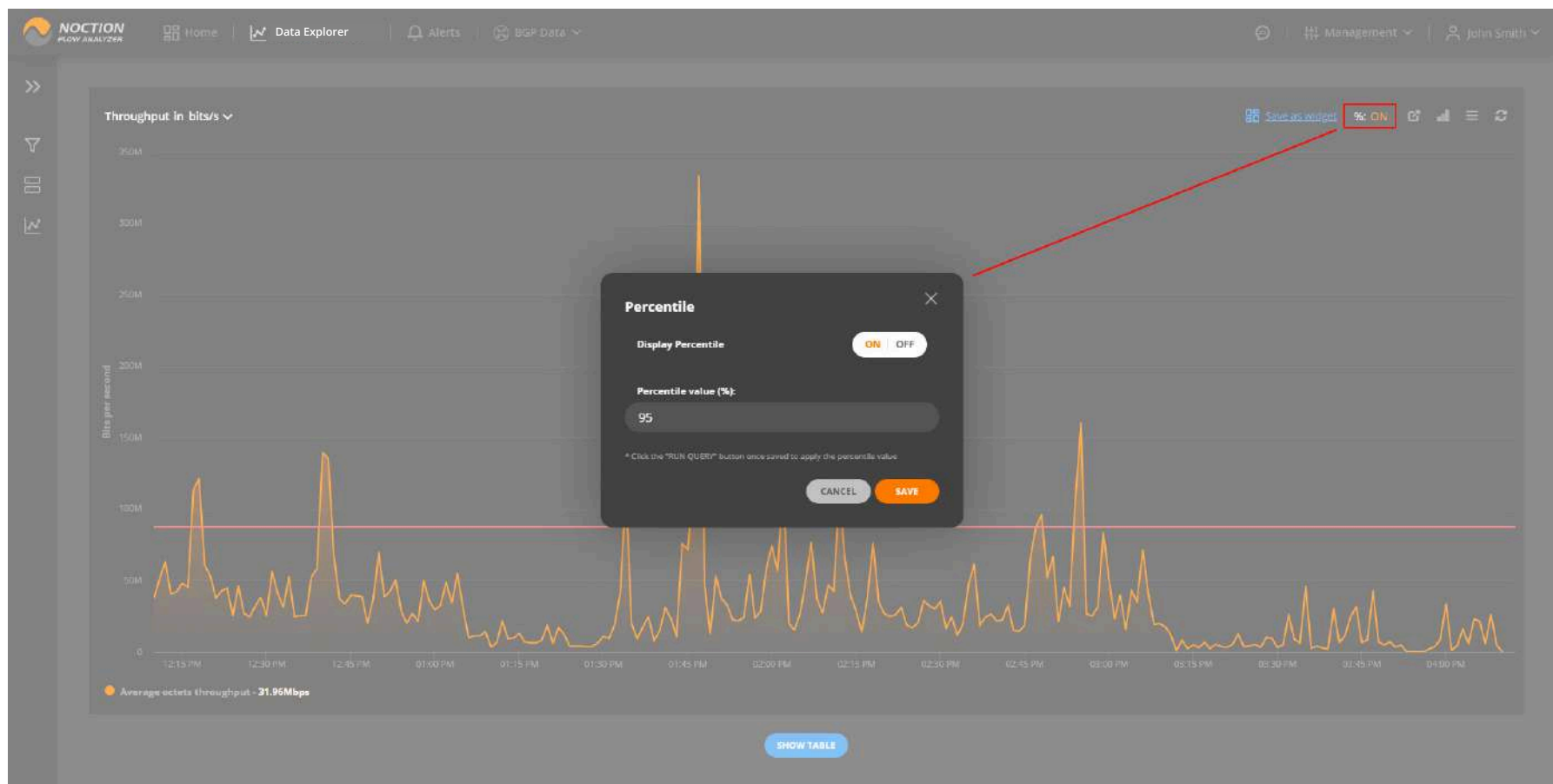
Time intervals govern how fast and how detailed the resulting data can be. When a query extends over a long time interval or checks data far in the past the results will be less granular compared to shorter and current time intervals.



## 2.2.5 Percentile Reporting

95th percentile is a popular network calculation used for reporting and billing burstable network usage. It typically serves as a baseline for traffic utilization metering on a network. Starting with NFA v 21.06, percentile value calculation, be it for 95th or any other, is available for packets, octets, and flows.

Go to **Data Explorer**, click the % icon, specify the percentile you want NFA to calculate, add any filtering conditions, and hit the **“Run Query”** button. Note, NFA calculates the Xth percentile, where X is an integer between 1 and 100. Feel free to save your view as a widget and add it to any of your dashboards.



## 2.3 BGP Data

BGP Data is delivered as an optional add-on to Noction Flow Analyzer.

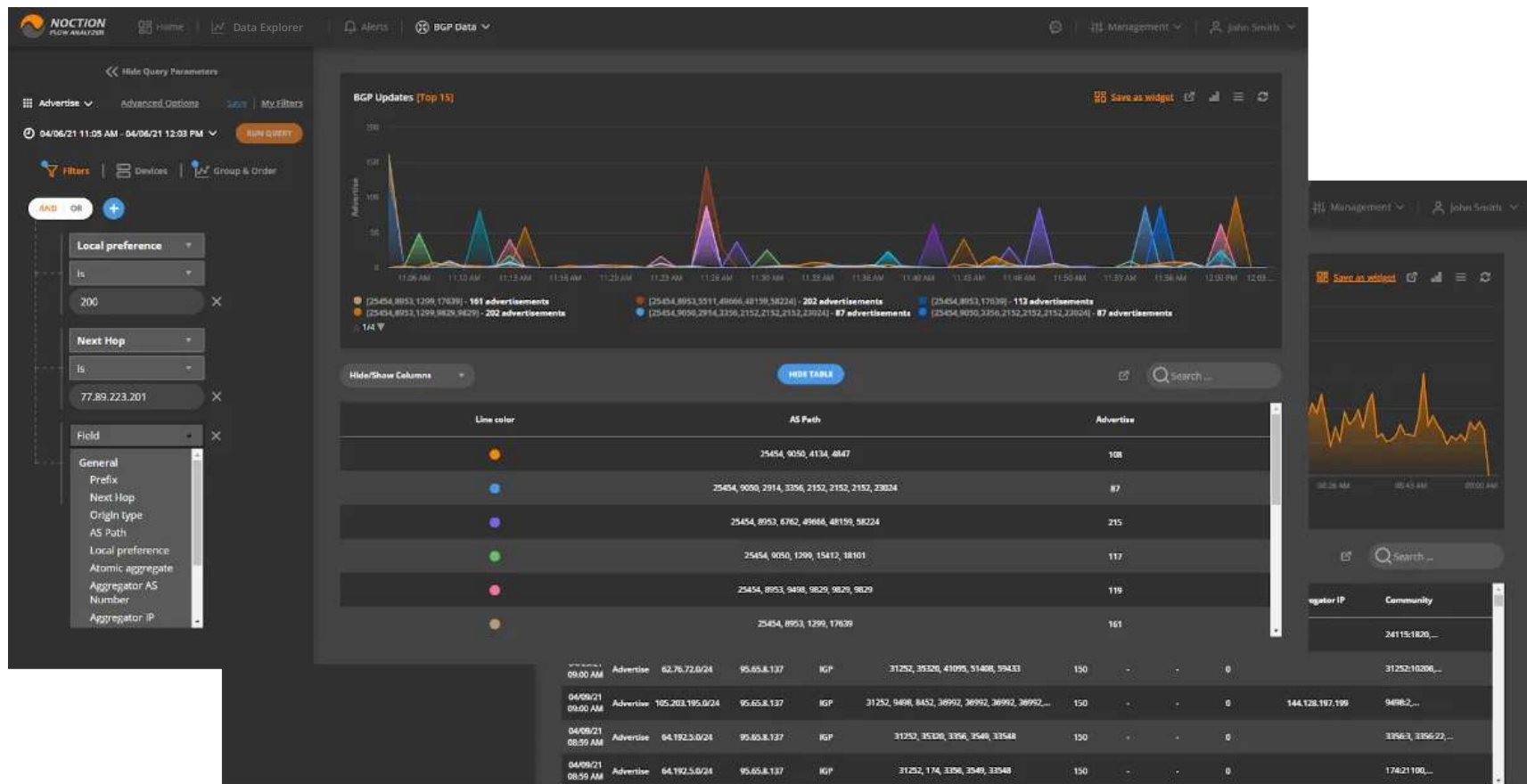
NFA overcomes the limitation of BGP support in traditional NetFlow. It employs a collection of full BGP data from BGP tables of edge routers, extracting the required BGP attributes. NFA extracts BGP attributes such as AS\_PATH and matches the obtained data with a corresponding flow record from Flow DB tables. This enables NFA to see and filter on the full BGP path, not just the next hop, first three or last three AS numbers.

Enabling BGP data will require you to establish a BGP session between at least one of your routers and NFA.

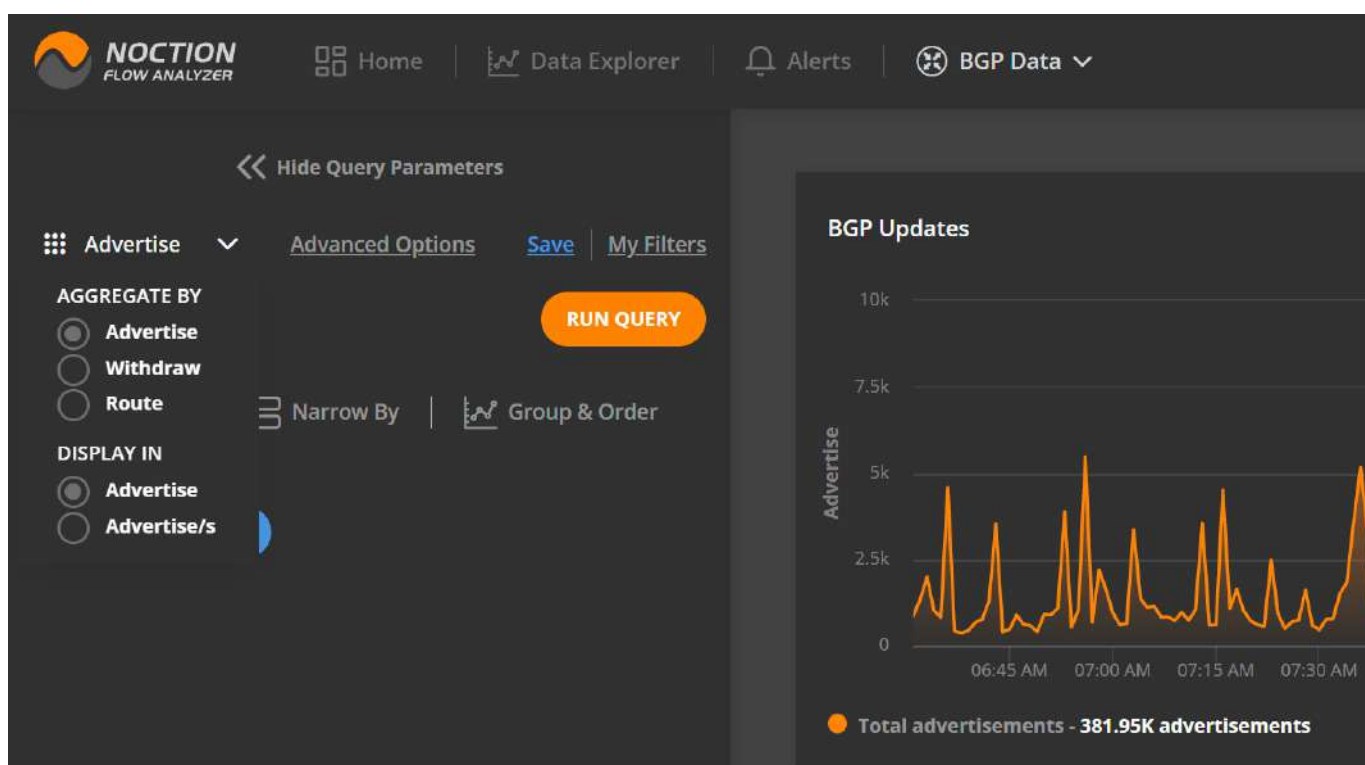
### 2.3.1 BGP Report

Use the BGP Report section to see BGP data obtained from your devices. The BGP Route advertisements and withdrawals can now be visualized both in a graph and table mode.

Filter, group, and search data according to your needs. Create and add custom widgets to any of your dashboards.



BGP Route advertisements and withdrawals can be visualized both in a graph and table mode. BGP Routes representation helps provide a greater view of prefix reachability inconsistency details obtained from the connected devices. Users can analyze the effect of routing changes by reviewing all routes active in the selected time window or filter results down to a specific prefix.

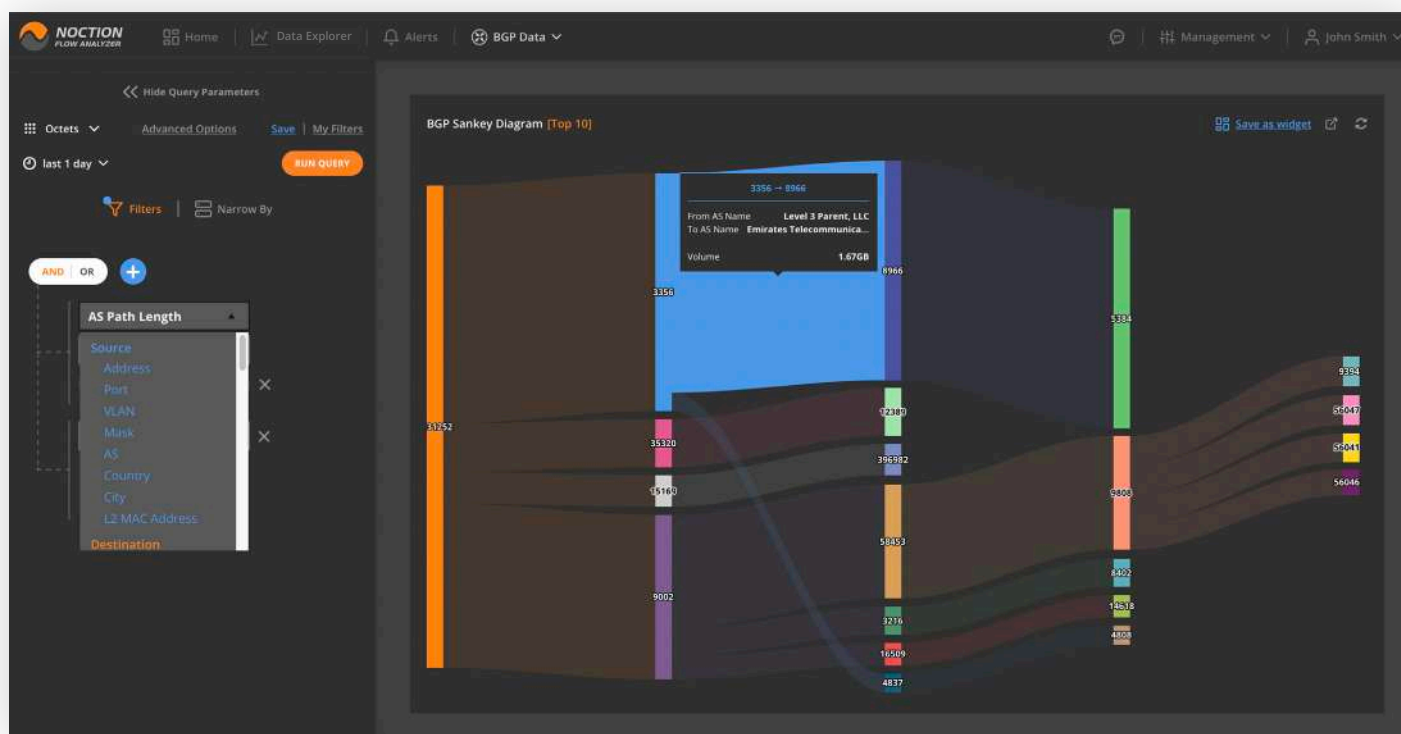


### 2.3.2 BGP Sankey Diagram

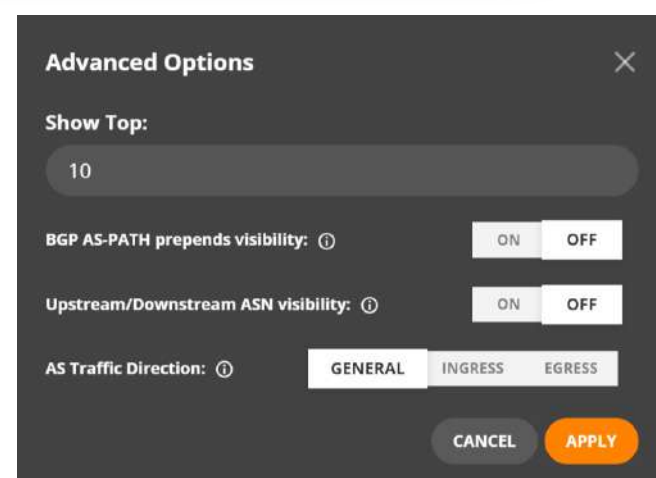
NFA offers a great way to visualize the Internet traffic routing criteria along with traffic volume using a Sankey type diagram. Its extensive filtering capabilities can provide you with a clear picture of the paths your traffic is taking, the countries regions or cities you traffic originates and terminates in, traffic volume distribution by different paths, best potential new peering candidates, and a lot more.

The list of available filters is listed below:

- Time
- Source and Destination Address
- Source and Destination Port
- Source and Destination VLAN
- Source and Destination Mask
- Source and Destination AS Number
- Source and Destination AS Path
- Source and Destination AS Path
- Source and Destination Country
- Source and Destination City
- Source and Destination L2 MAC Address
- MPLS Top Label to Top Label 9
- MPLS Top Label Type
- MPLS Top Label IPv4 Address
- MPLS Top Label IPv6 Address
- MPLS Top Label Prefix Length
- MPLS VPN Route Distinguisher
- MPLS Top Label TTL
- MPLS Label Stack Length
- MPLS Label Stack Depth
- MPLS Top Label Exp
- L3 IP TTL
- L3 IP min TTL
- L3 IP max TTL
- L3 IP Total Length
- L3 IP min Total Length
- L3 IP max Total Length
- BGP Community
- TOS - Type of Service
- Protocol
- Input Interface
- Output Interface
- Next Hop Address
- Pseudowire ID
- Pseudowire Type
- Pseudowire Control Word
- BGP Local Preference
- BGP MED
- L2 Ethernet Type
- Exporter Address
- Exporter ID
- TCP Flag
- Flow Role
- Length
- Exporter AS
- Application Name
- Application Name Custom Group
- Application Name Length
- Source and Destination FQDN address



Click “**Advanced Options**” to increase/decrease the number of BGP paths visible on the diagram, show/hide the AS path preponds as well as the upstream/downstream ASNs info, and select the Ingress, Egress, or a combined view of the AS traffic.

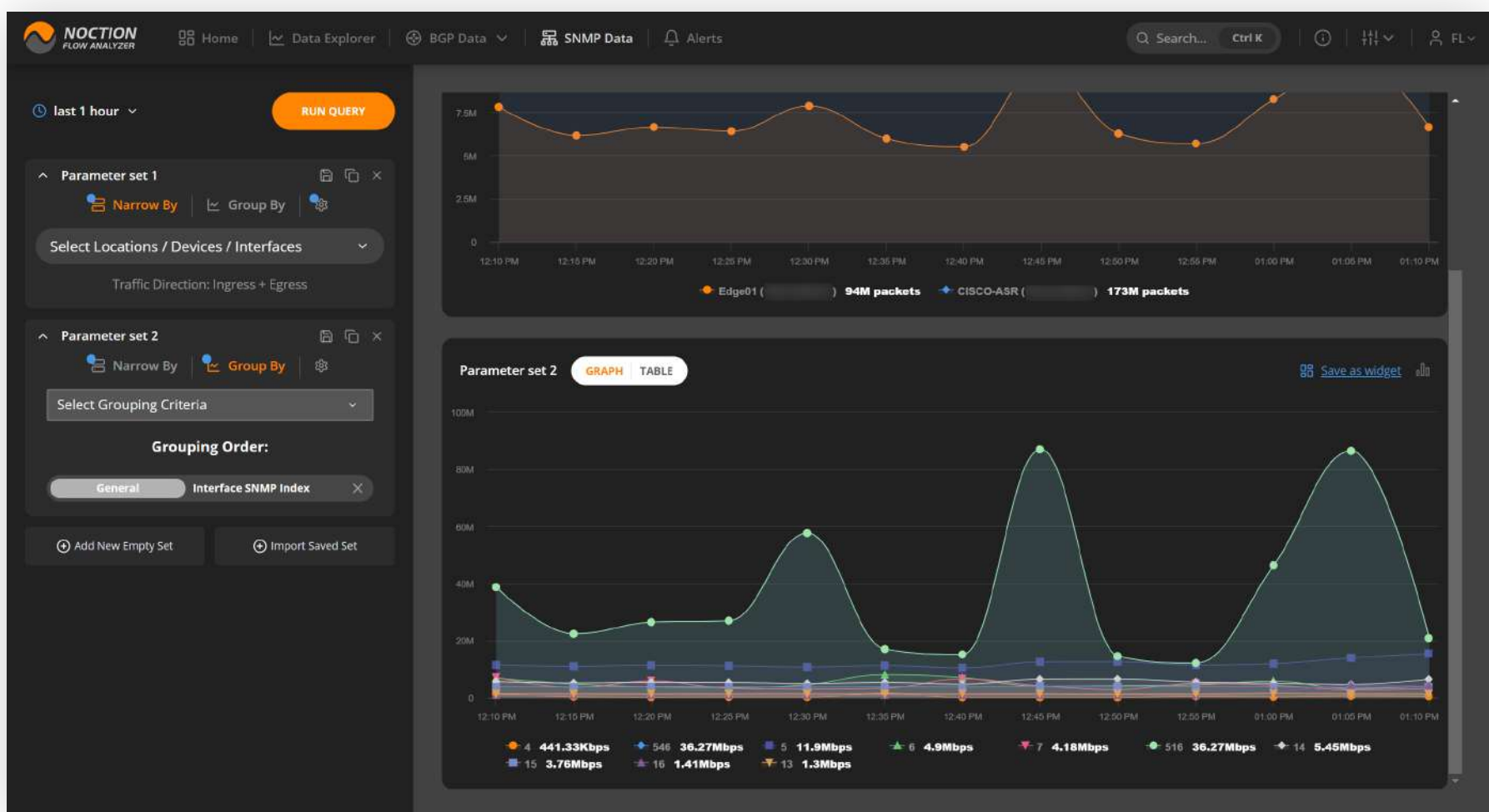


## 2.4 SNMP Data

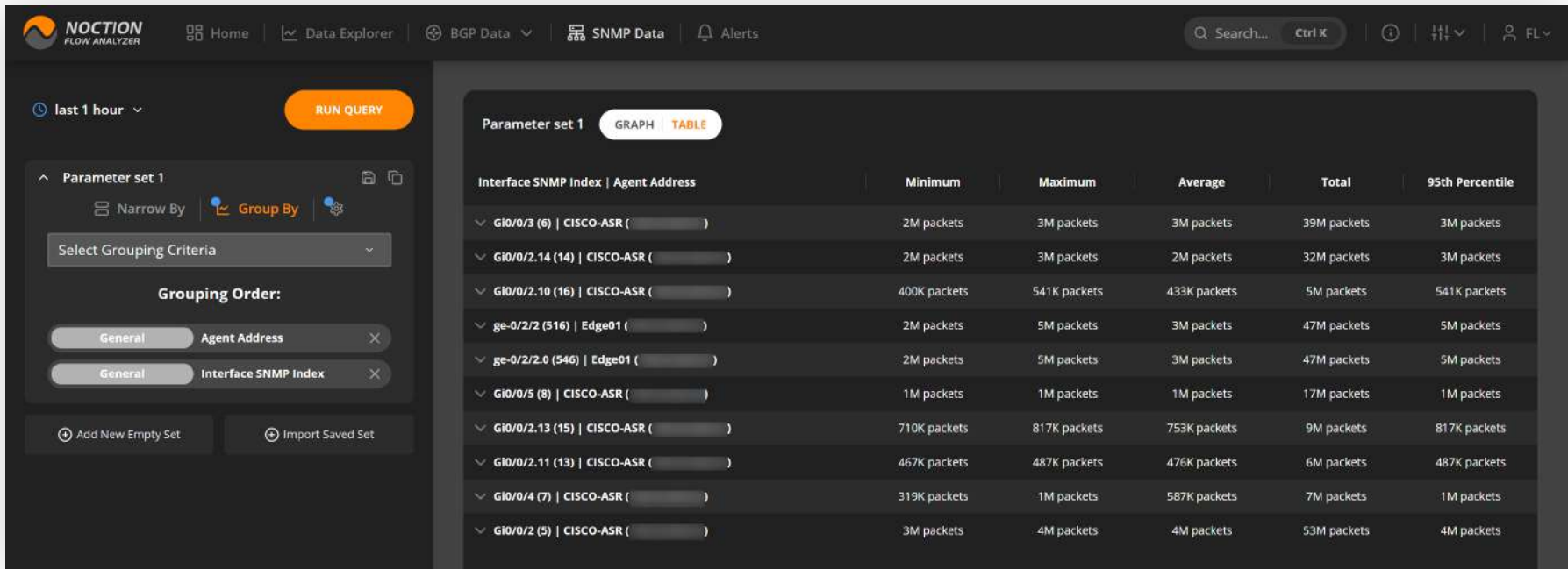
SNMP Data provides detailed network traffic stats in both graph and table formats. Make sure the SNMP v2c or v3 details are provided for the Devices of interest under the **Inventory section**. **“Narrow By”** Locations, Devices, or Interfaces and **“Group By”** Agent Address and/or Interface SNMP Index to focus or broaden attention to the desired aspects of network traffic.

SNMP Data Explorer can be accessed either from the Main Menu or by clicking on any widget’s header on dashboards containing the “SNMP” tag. Any grouping and narrowing by criteria previously set up in widgets will auto-populate in SNMP Data Explorer.

SNMP Explorer supports the addition and execution of multiple parameter sets simultaneously. This allows users to input several SNMP parameters and run them concurrently, streamlining the monitoring process and providing a more comprehensive view of network performance. Parameter sets can be renamed / saved and imported later on when required.

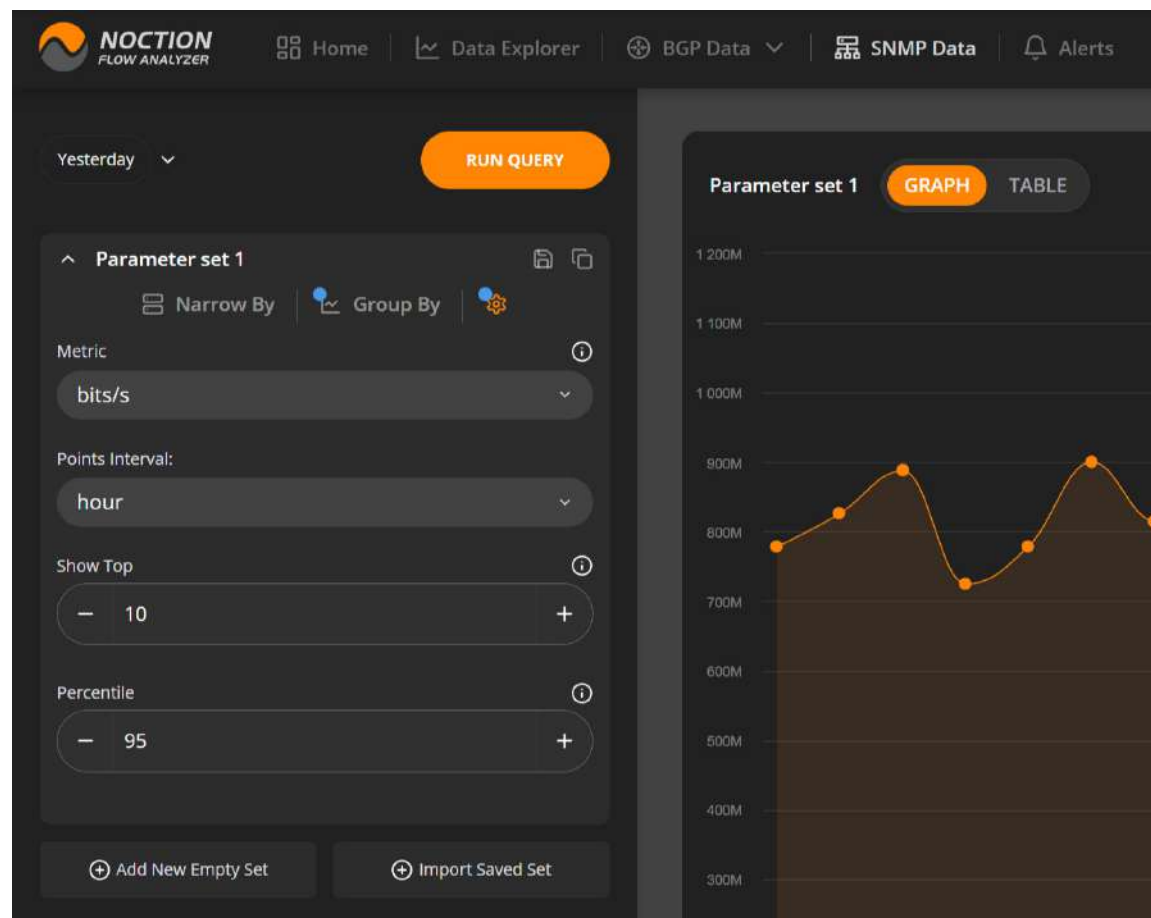


The table view can facilitate quicker decision-making based on SNMP metrics.



Click the **Gear icon** to open up Settings for a specific Parameter Set. Select the desired metric to be displayed. Choose the points interval for the graph, e.g. auto, hour, day, week, etc. You can also limit the graph/table to show the desired top N results (top 10 is the default value) for a simplified and more focused data visualization.

Additionally, we can specify the number of values to be displayed in both the table and the graph in Show Top field (by default 10).



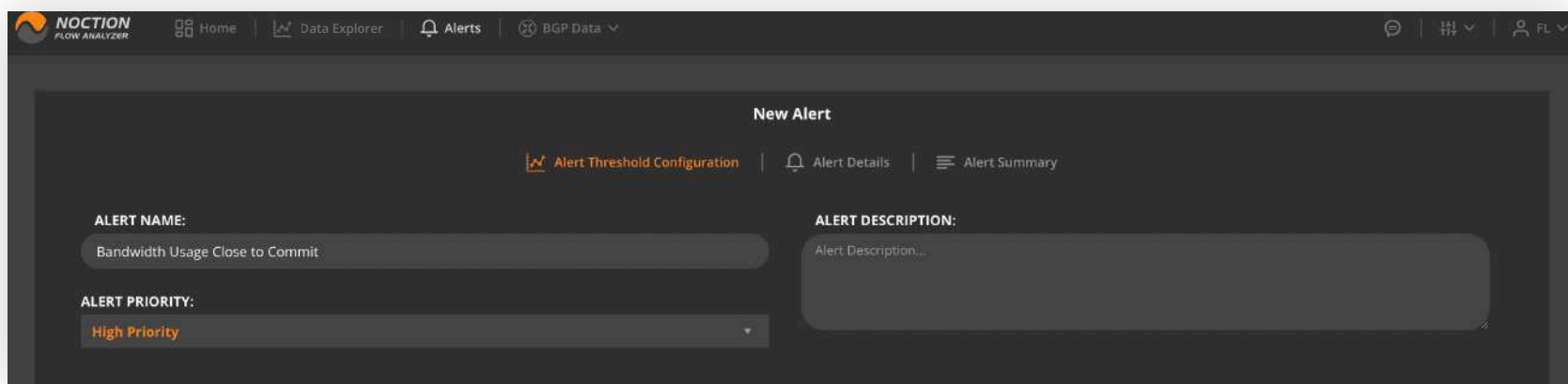
A functionality for SNMP includes the ability to specify percentile, which is then visualized as a plotline on the graph, providing a clear representation of the percentile distribution. The advantage of using percentiles in SNMP monitoring is that it allows for a more nuanced view of network performance by highlighting data distribution rather than just average or peak values.

## 2.5 Alerts

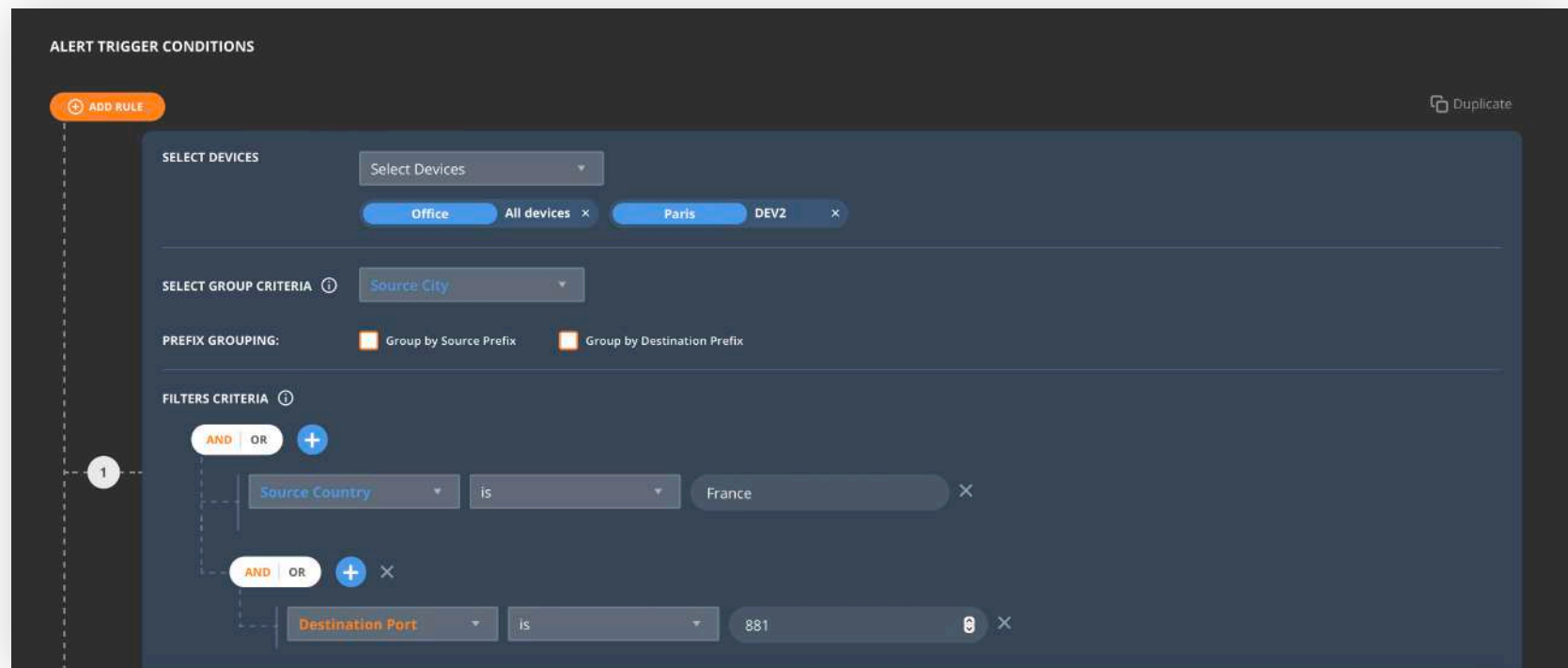
NFA lets you set up a robust and customizable alert system that can proactively notify you when important conditions are detected in your network traffic data. You can configure alerts based on different characteristics and parameters of your network traffic: volume changes, frequency, specific traffic type existence, duration, baseline or a complex combination of such characteristics.

### 2.5.1 Creating Alerts

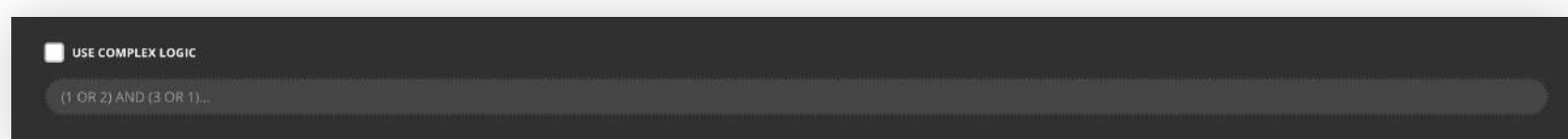
1. Go to **Alerts > My Alerts** and click the **“Create New Alert”** button.
2. Enter a meaningful **Name** and **Description** for the Alert. Select an appropriate Priority Level: **Low, High** or **Critical**.



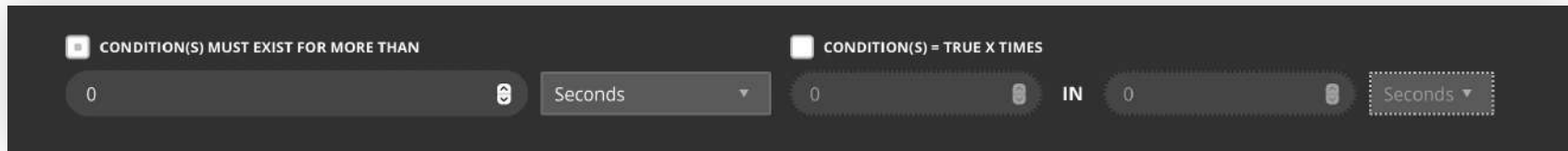
3. Specify Alert Trigger Conditions by adding a single or multiple trigger **Rules**.



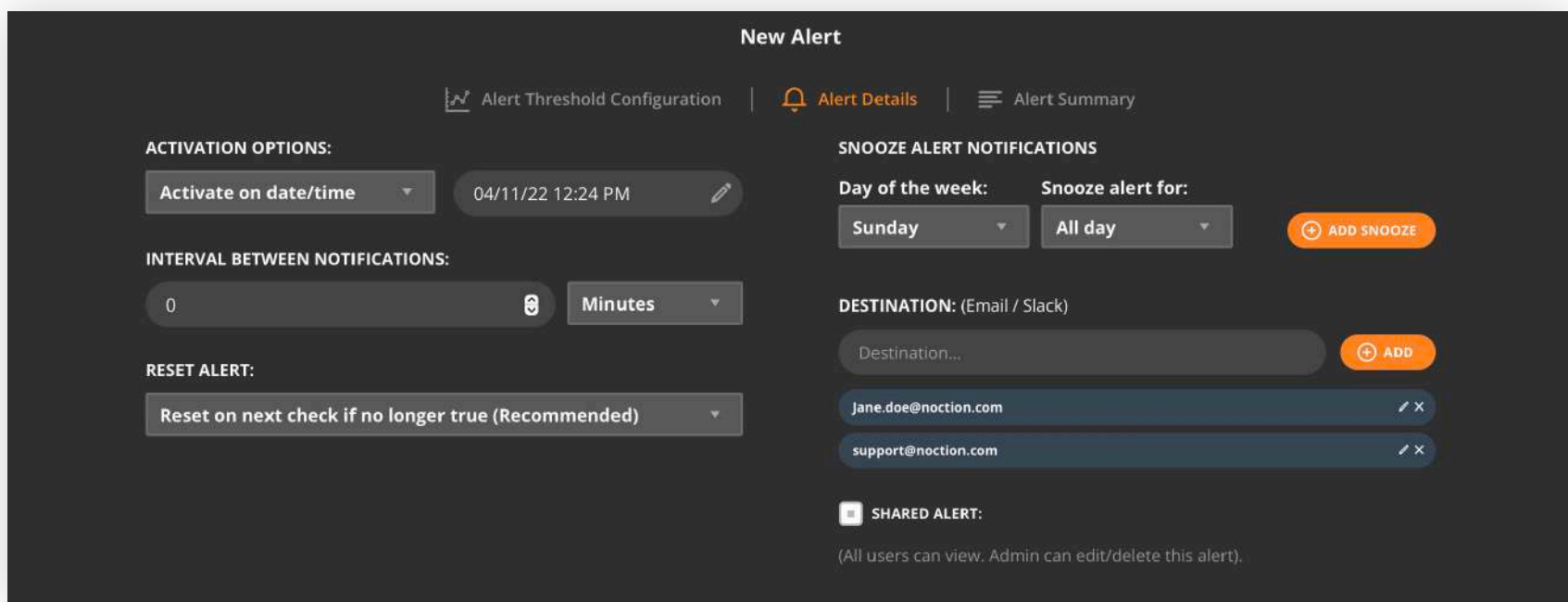
When setting up numerous Rules with complex logic, checkmark and fill out the corresponding **“Use Complex Logic”** field. Hit **Apply**.



- When relevant, checkmark and indicate the time interval during which the condition should exist for an Alert Notification to be sent. Alternatively, checkmark and specify the number of times an alert condition should change its state to "True" (e.g. Abnormal traffic behavior detection scenario) within a specific time interval for the Alert Notification to be sent. Proceed to **Next Step**.



- On the Alert Details page, select if you'd like the alert to be activated immediately or at a later date/time. Indicate the time interval between notifications, alert reset conditions and snooze options to reduce alert fatigue.



- Indicate email(s) or Slack channel you'd like the Alert Notifications to be sent to and proceed to the **Next Step**.

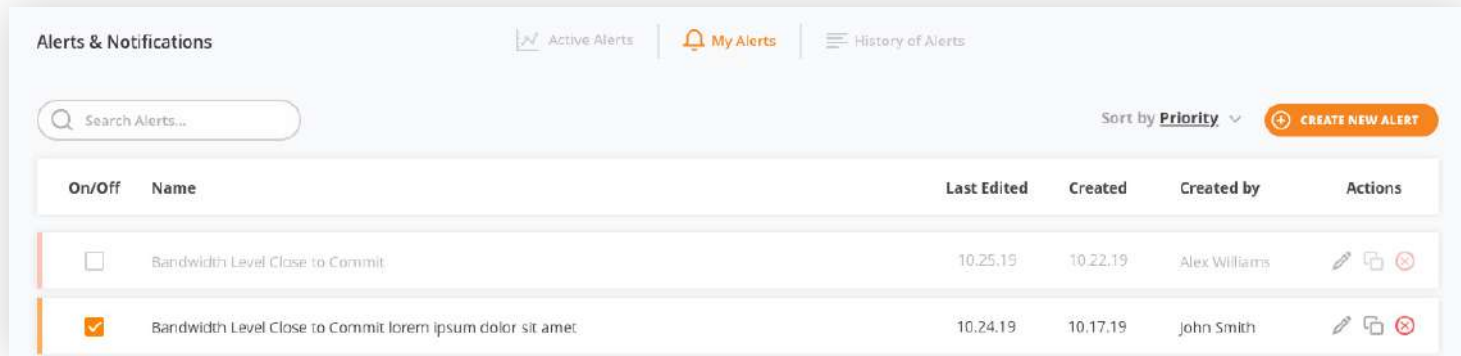
**Note:** The notification channels must be properly set up from the Management > System Notifications > Notification Channels section for users to receive alert notifications.

- Review your Alert details, Notification Channels and **Save Alert**.



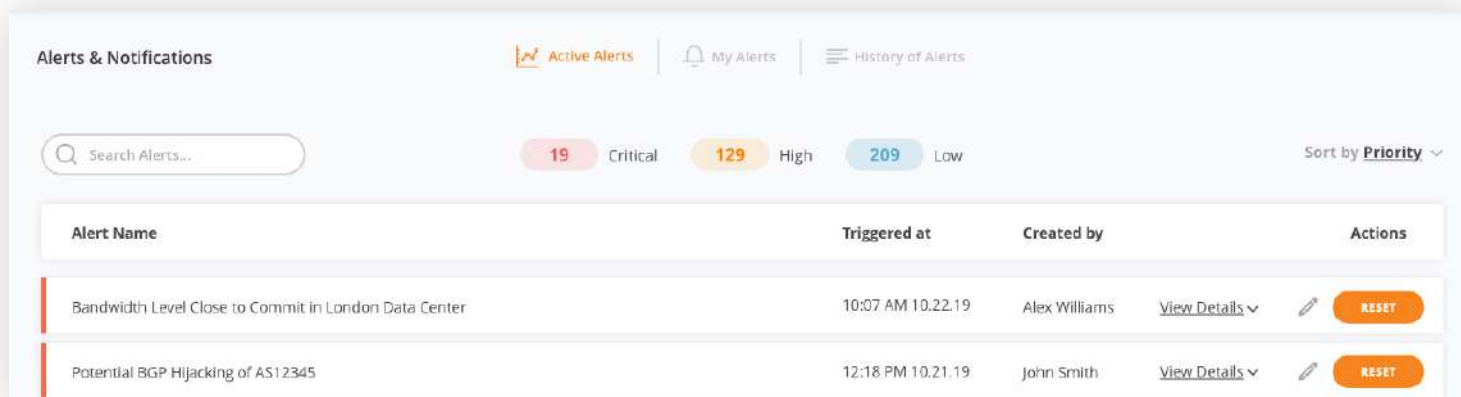
## 2.5.2 My Alerts

My Alerts section contains a list of Alerts that have been created by your NFA users. Depending on the user access level you can edit, duplicate, delete alerts or turn them on/off.



## 2.5.3 Active Alerts

Active Alerts section allows you to view the triggered alert details, triggered alert date/time, and allows you to reset (acknowledge) alerts.



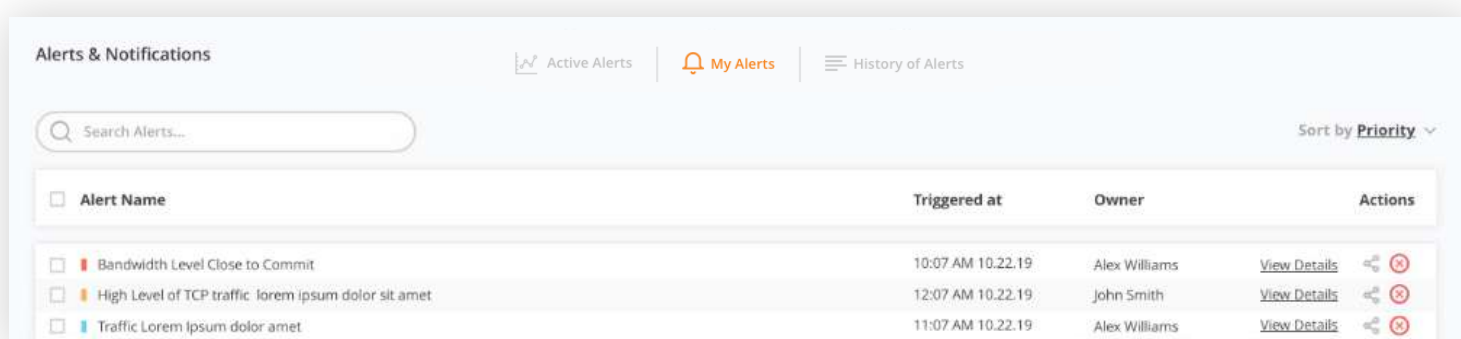
**Note:** When you reset (acknowledge) an alert you are taking ownership of it. This means you are aware of the conditions which triggered an alert and are taking action to solve the issue.

Follow your company’s guidelines on further actions once you acknowledge/reset a triggered alert. Acknowledged/Reset triggered alerts will be flagged with your user name and moved to the **History of Alerts** section.

All triggered alerts in NFA show up with UTC timestamps. This is specifically useful for teams using NFA from multiple geographical time zones.

## 2.5.4 History of Alerts

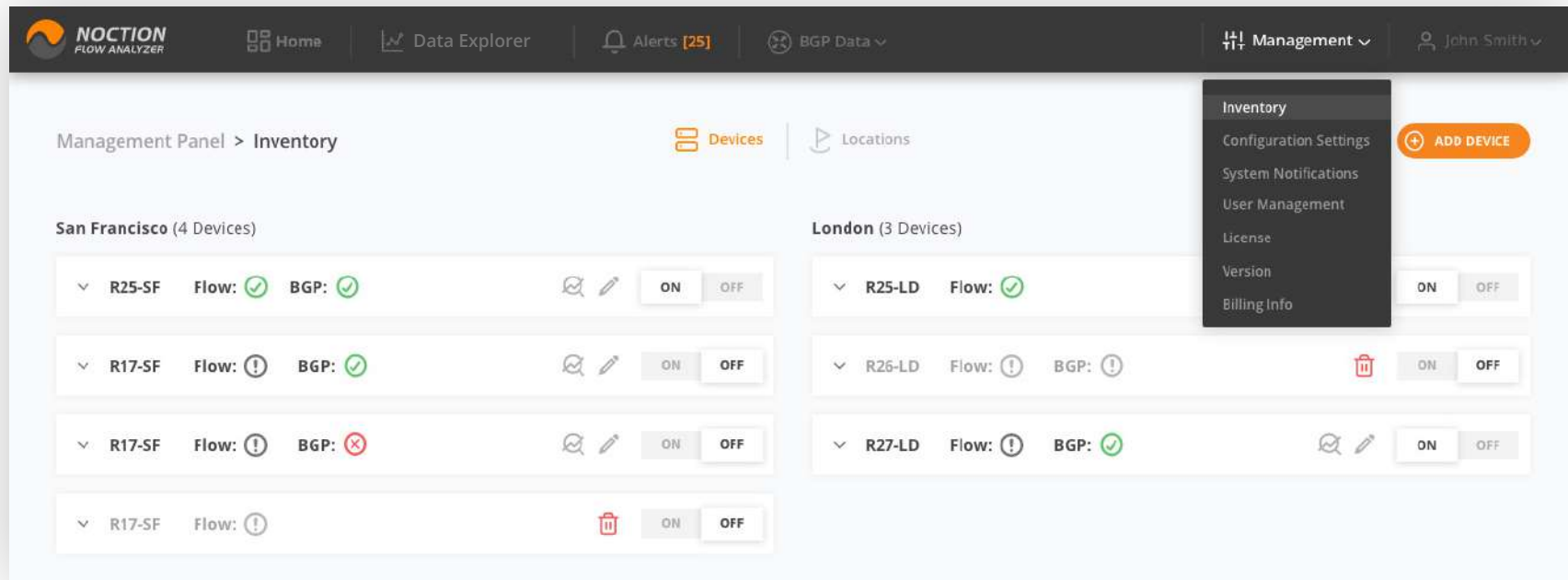
All triggered alerts are saved in the **History of Alerts** section. Use the available options to search and sort the alert incidents.



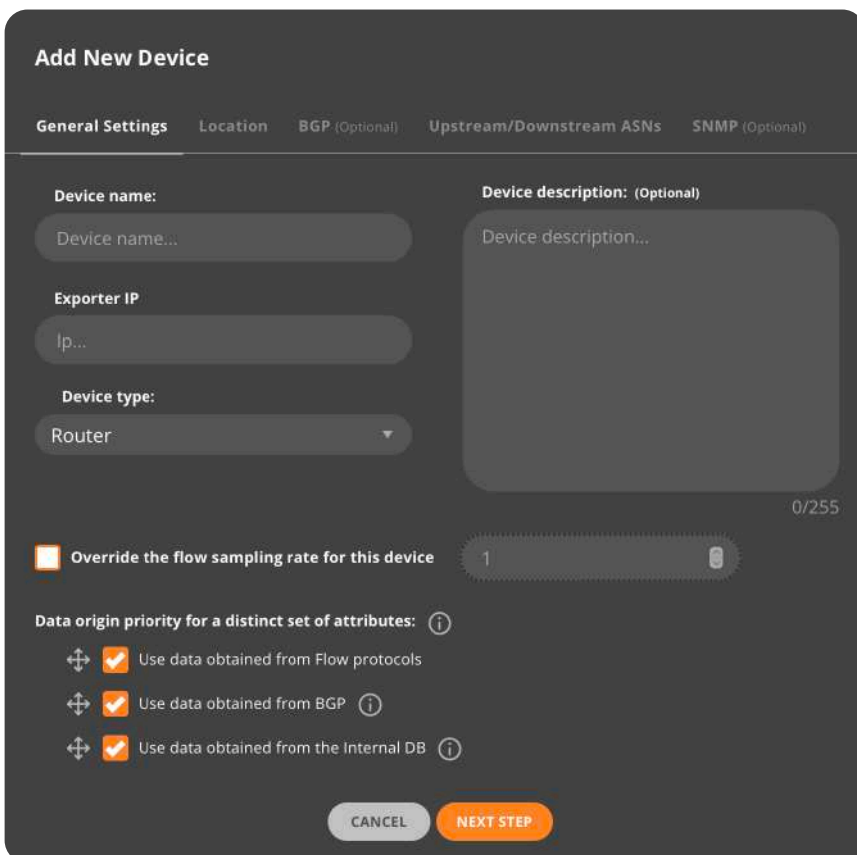
### 3. Management

#### 3.1 Inventory

The Inventory section accumulates information about all types of network devices being used in NFA and assigns them meaningful names. Devices must be assigned to locations/sites to further enhance NFA’s grouping and filtering capabilities.

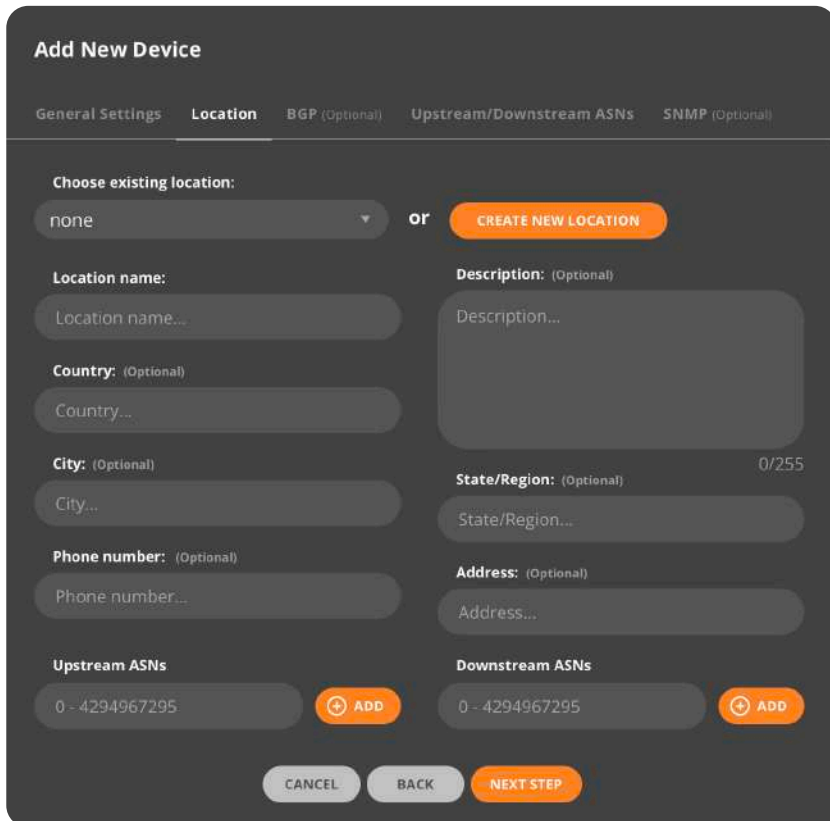


##### 3.1.1 Adding Devices



To add a new device, go to **Management > Inventory**. Click the **“ADD DEVICE”** button in the top right corner. A dialog box will appear and ask to provide the following information: Device Name, Device Description, Device Type, and Exporter IP.

Specify if you’d like to override the flow sampling rate for the device you are adding. Define and set up the data origin (Flow, BGP, or the Internal Database) priority for a distinct set of attributes. Click **“NEXT STEP”** to proceed.



**Add New Device**

General Settings | **Location** | BGP (Optional) | Upstream/Downstream ASNs | SNMP (Optional)

Choose existing location:  
 none  or

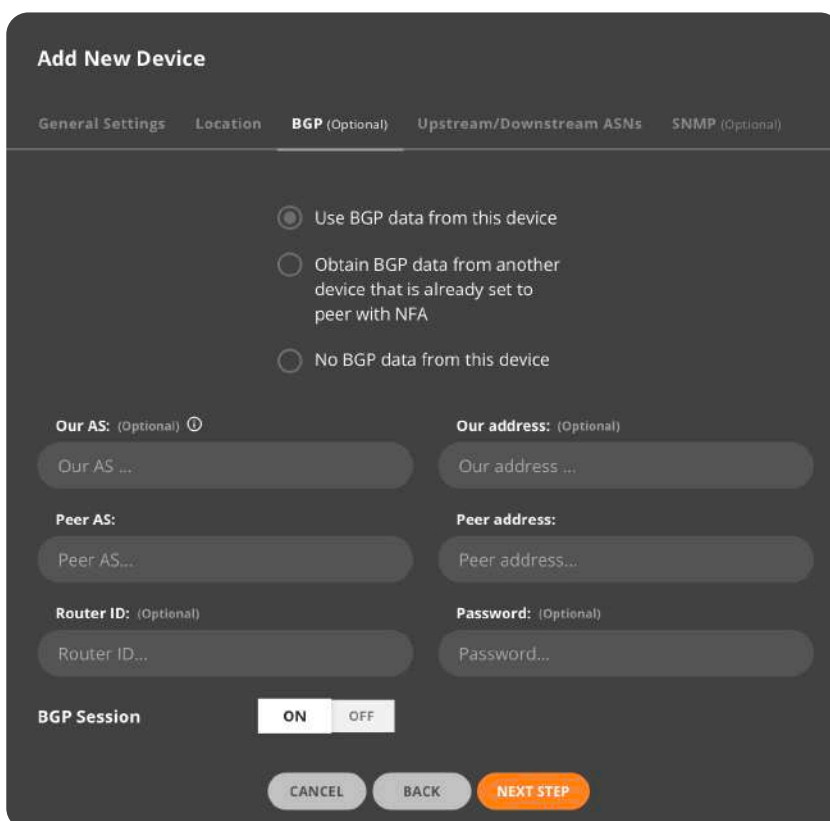
Location name:   
 Description: (Optional)

Country: (Optional)   
 City: (Optional)  0/255  
 State/Region: (Optional)

Phone number: (Optional)   
 Address: (Optional)

Upstream ASNs   Downstream ASNs

Select an existing location for your device from the dropdown menu or choose to “Create New Location”. Proceed to the “**NEXT STEP**”



**Add New Device**

General Settings | Location | **BGP (Optional)** | Upstream/Downstream ASNs | SNMP (Optional)

Use BGP data from this device  
 Obtain BGP data from another device that is already set to peer with NFA  
 No BGP data from this device

Our AS: (Optional)  Our address: (Optional)   
 Peer AS:  Peer address:

Router ID: (Optional)  Password: (Optional)

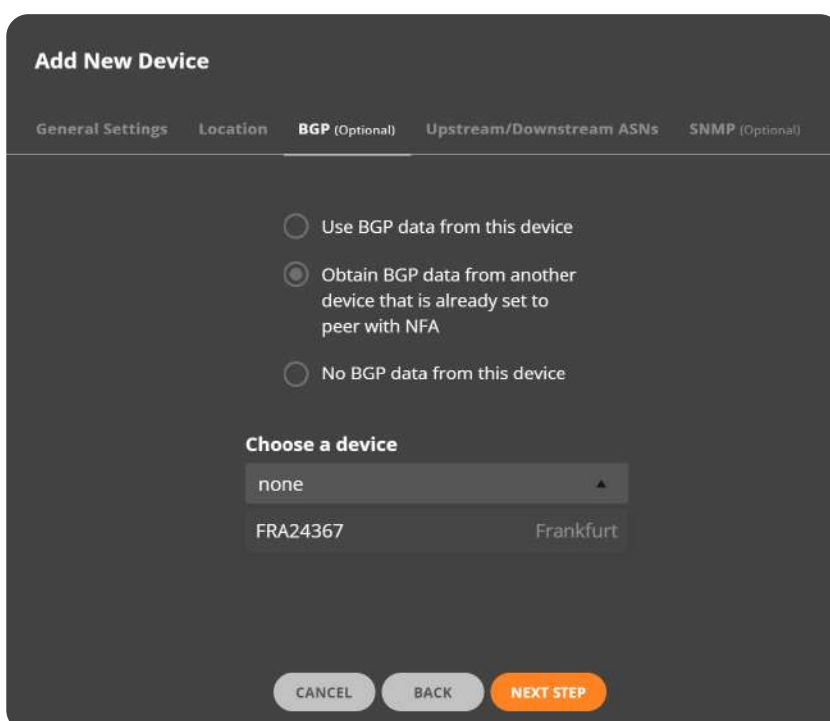
BGP Session  ON  OFF

Enabling BGP data export from the device you are about to add is optional.

First, configure an iBGP or eBGP session between NFA and your router(s).

Next, fill out both **OUR AS** and **PEER AS** fields under the BGP settings tab for eBGP. With eBGP, the route-reflector does not need to be configured, and the router side just needs to be set up as though it’s a transit customer. If **OUR AS** field is left blank, an iBGP session will be established.

The BGP SESSION control is set to ON by default.



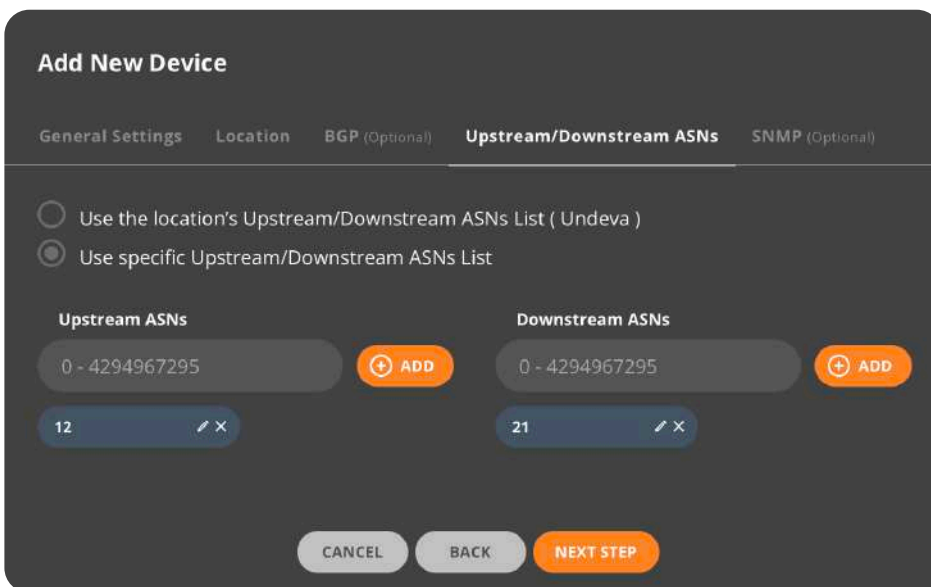
**Add New Device**

General Settings | Location | **BGP (Optional)** | Upstream/Downstream ASNs | SNMP (Optional)

Use BGP data from this device  
 Obtain BGP data from another device that is already set to peer with NFA  
 No BGP data from this device

Choose a device  
  
 FRA24367 Frankfurt

NFA allows you to use the BGP data from another device that is already set to peer with NFA. For this to happen, select the corresponding radio button and an existing device from the dropdown list. Proceed to the “**NEXT STEP**”



**Add New Device**

General Settings | Location | BGP (Optional) | **Upstream/Downstream ASNs** | SNMP (Optional)

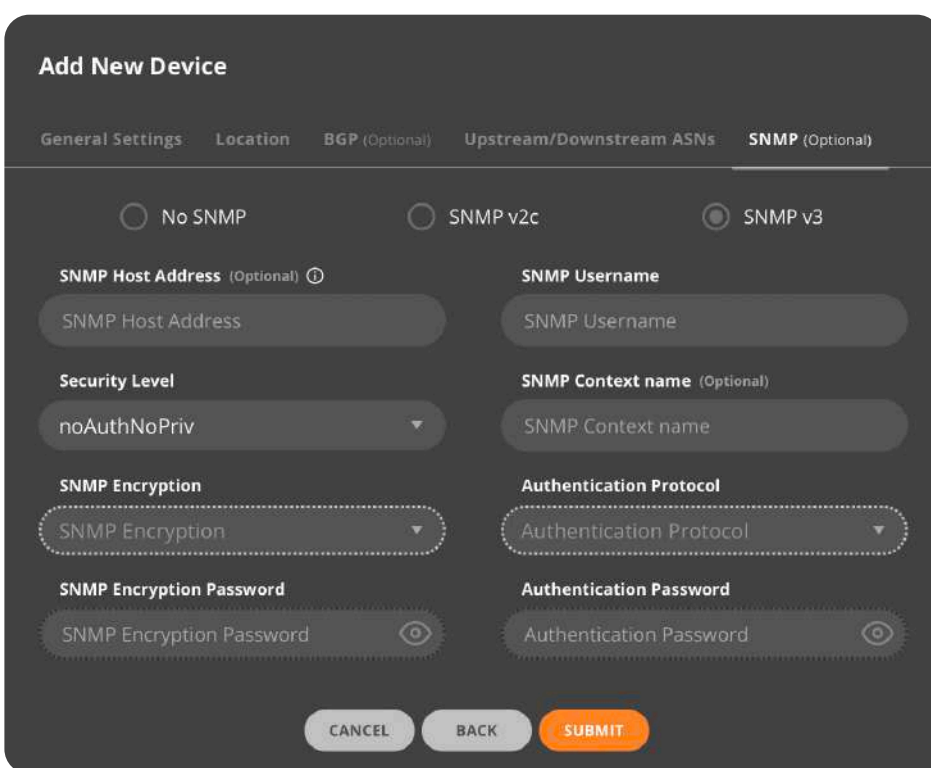
Use the location's Upstream/Downstream ASNs List ( Undeva )  
 Use specific Upstream/Downstream ASNs List

**Upstream ASNs**  
 0 - 4294967295 + ADD  
 12 ✕

**Downstream ASNs**  
 0 - 4294967295 + ADD  
 21 ✕

CANCEL | BACK | **NEXT STEP**

Feel free to indicate a list of upstream/downstream ASNs specific to your network. The user-defined upstream/downstream lists can be set for each device individually or per a particular location.



**Add New Device**

General Settings | Location | BGP (Optional) | Upstream/Downstream ASNs | **SNMP (Optional)**

No SNMP |  SNMP v2c |  SNMP v3

**SNMP Host Address (Optional)**  
 SNMP Host Address

**SNMP Username**  
 SNMP Username

**Security Level**  
 noAuthNoPriv

**SNMP Context name (Optional)**  
 SNMP Context name

**SNMP Encryption**  
 SNMP Encryption

**Authentication Protocol**  
 Authentication Protocol

**SNMP Encryption Password**  
 SNMP Encryption Password

**Authentication Password**  
 Authentication Password

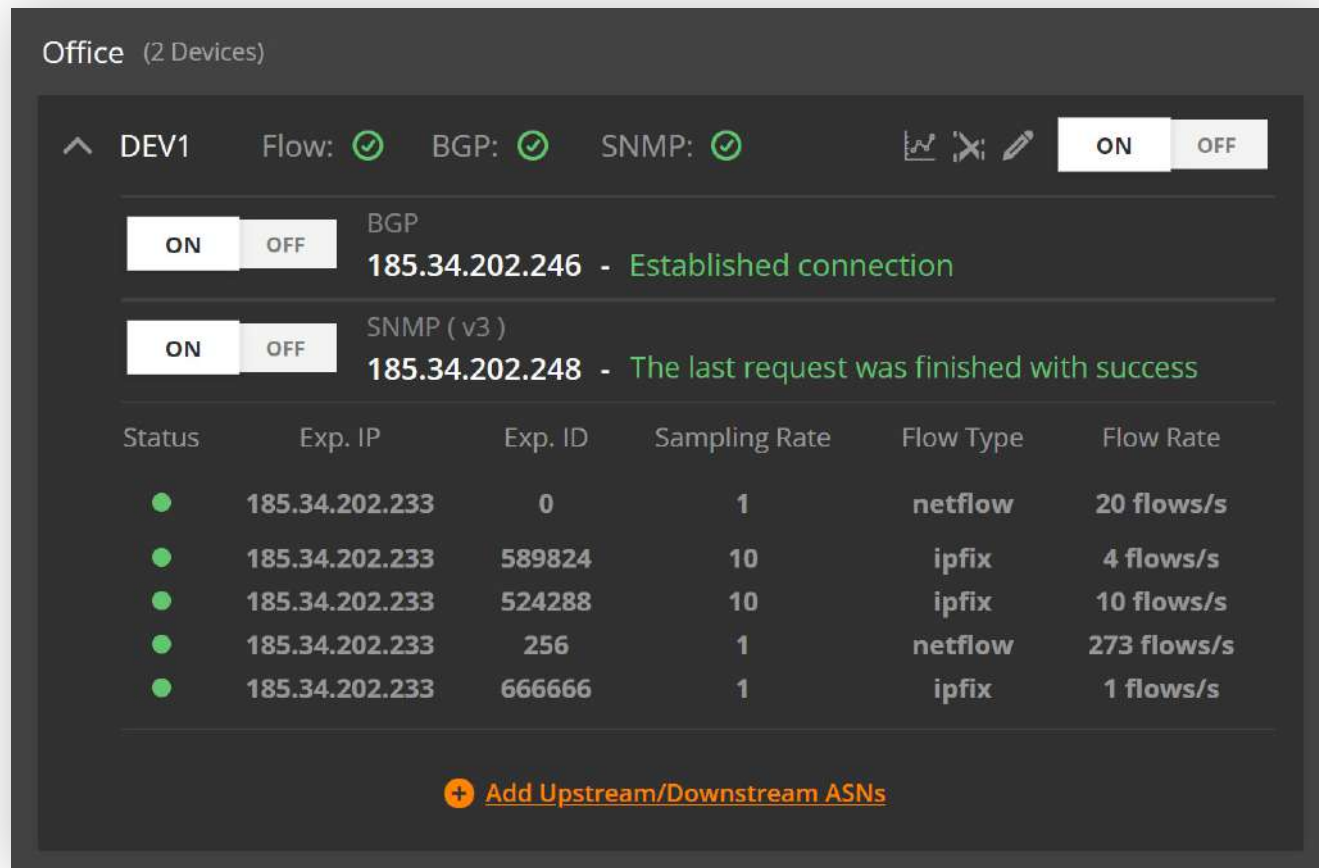
CANCEL | BACK | **SUBMIT**

Provide optional SNMP details for NFA to be able to poll any device that supports MIB-II (a standard MIB), get interface names and descriptions, and monitor bandwidth usage on each interface.

Both SNMPv2c and SNMPv3 can be defined. Since SNMPv3 supports authentication and encryption, we recommend using this version when possible. Once set up, interface names and descriptions will appear as the “narrow by” options in NFA’s Data Explorer section.

### 3.1.2 Managing Devices

All devices added to NFA are listed under **Management > Inventory**. Devices are grouped by location. Small icons next to Flow, BGP and/or SNMP indicate their state. Click a small arrow next to the device name to see the additional information such as the Exporter IP, Sample rate, Flow type and Flow rate or turn **ON/OFF** the BGP session or SNMP.



Office (2 Devices)

DEV1 Flow: ✔ BGP: ✔ SNMP: ✔ ON OFF

ON OFF BGP  
185.34.202.246 - Established connection

ON OFF SNMP (v3)  
185.34.202.248 - The last request was finished with success

Status	Exp. IP	Exp. ID	Sampling Rate	Flow Type	Flow Rate
<span style="color: green;">●</span>	185.34.202.233	0	1	netflow	20 flows/s
<span style="color: green;">●</span>	185.34.202.233	589824	10	ipfix	4 flows/s
<span style="color: green;">●</span>	185.34.202.233	524288	10	ipfix	10 flows/s
<span style="color: green;">●</span>	185.34.202.233	256	1	netflow	273 flows/s
<span style="color: green;">●</span>	185.34.202.233	666666	1	ipfix	1 flows/s

+ Add Upstream/Downstream ASNs

Note: All devices exporting data to the system but not yet registered by admins are automatically placed under the default “Unregistered” category. These can be named, edited and registered as per your requirements.

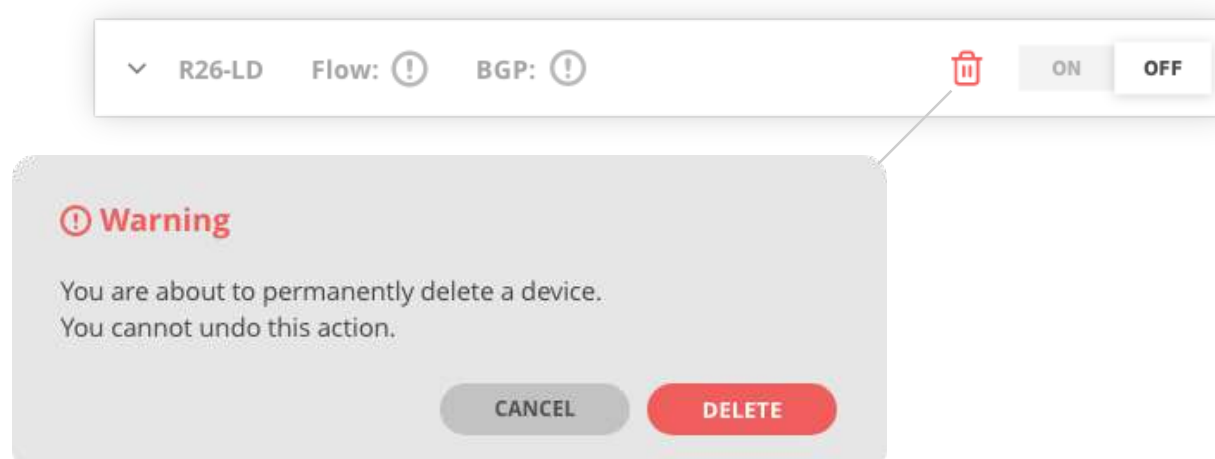


Unregistered (1 Devices)

Flow: ⊗ REGISTER

### 3.1.3 Deleting Devices

To delete a device you’ll need to deactivate it first. Click the OFF switch for a particular device. Next, click the delete icon. A dialog box will appear asking you to confirm the deletion.



R26-LD Flow: ! BGP: ! ON OFF

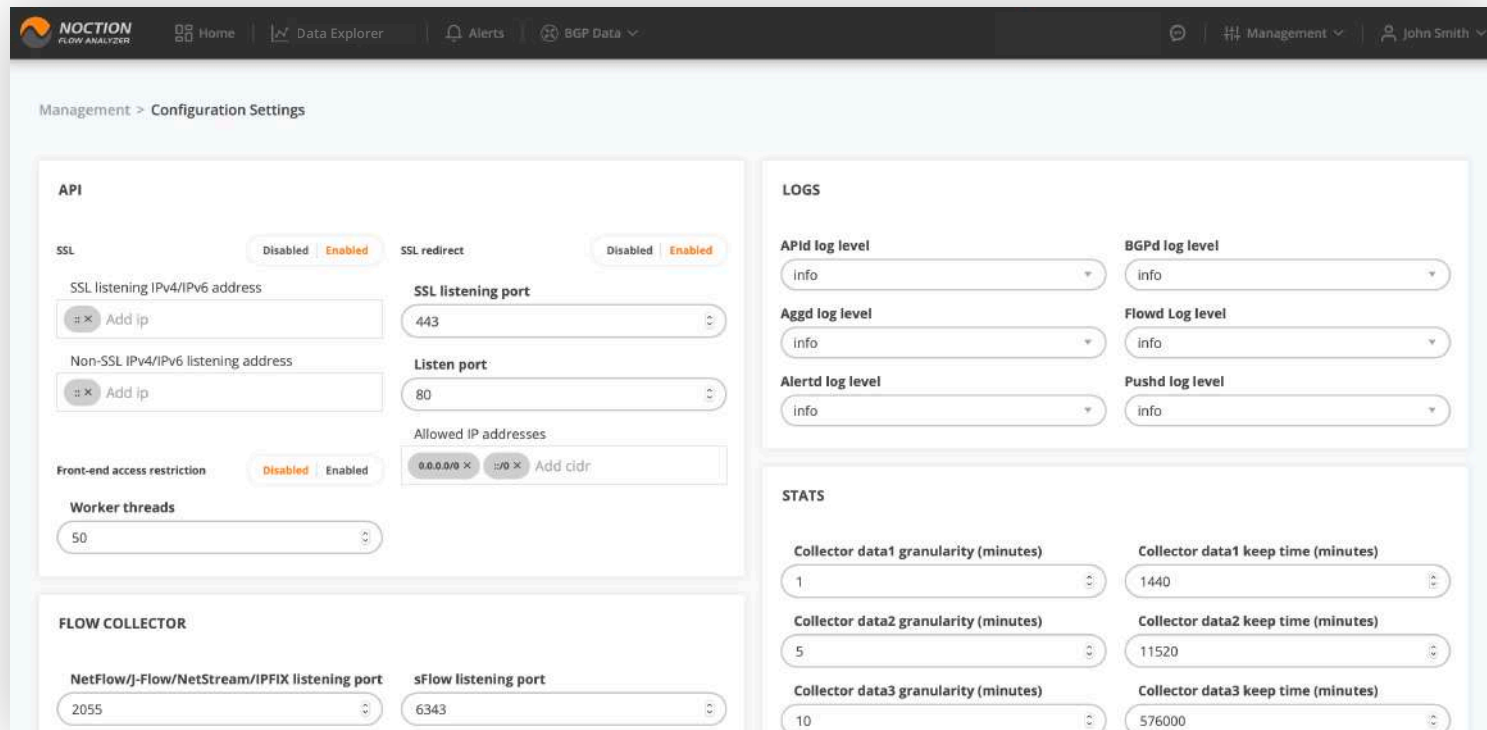
! **Warning**

You are about to permanently delete a device.  
You cannot undo this action.

CANCEL DELETE

## 3.2 Configuration Settings

NFA has a large set of configuration settings available in the front end to fine-tune the system's behavior.



All parameters are preset with the default values and are organized in groups:

### API:

- **SSL** - Enables/disables SSL support
- **SSL Redirect** - Enables/disables SSL redirect from a non-SSL port
- **SSL listening IPv4/IPv6 address** - SSL (HTTPS) listening IPs
- **SSL listening port** - SSL (HTTPS) listening port
- **Non-SSL IPv4/IPv6 listening address** - Non-SSL (HTTP) listening IPs
- **Non-SSL listening port** - Non-SSL (HTTP) listening port
- **Front-end access restriction** - Enables/disables NFA front-end access restriction
- **Allowed IP addresses** - Lists the IPs or Subnets with access to the NFA frontend

### Flow Collector:

- **NetFlow/J-Flow/NetStream/IPFIX listening port** - Port on which the collector listens for NetFlow/J-Flow/Netstream/IPFIX packets.
- **sFlow listening port** - Port on which collector listens for sFlow packets
- **Buffer size (packets)** - The incoming packets buffer size
- **Flow stream stop event threshold (seconds)** - If flows stream was stopped, it defines the period of time after which FlowStreamStop event would be sent.
- **Extended exporter address determination logic** - Enables/Disables extended exporter address determination logic using IPFIX/NetFlow informations elements: 403:originalExporterIPv4Address, 404:originalExporterIPv6Address, 130:exporterIPv4Address, 131:exporterIPv6Address
- **BGP attributes Caching** - Enables/Disables BGP attributes caching
- **BGP Attributes cache size (in number of entries)** - Specifies the maximum number of cache entries in BGP attributes requester cache
- **BGP attributes cache TTU (Time to Use)** - Specifies the maximum number of seconds for TTU in BGP attributes requester cache of an entry

- **BGP attributes related requests timeout (milliseconds)**
- **Accept flow records from enabled devices only** - when enabled, NFA accepts flow records sent by exporter IP of the configured devices only
- **Enable triggering of DNS PTR records lookup** - enables/disables DNS PTR records lookup for the IP flow source and destination addresses.

### BGP:

- **KeepAlive message interval (seconds)** - The interval between two consecutive BGP keepalive messages
- **Hold time interval (seconds)** - Specifies how long NFA will wait for incoming BGP messages before it assumes the neighbor is dead.

### LOGS:

- **APId log level** - Specifies the log level for APId. The drop-down menu lists log levels in order, from most severe to least severe ones.
- **Flowd log level** - Specifies the log level for Flowd. The drop-down menu lists log levels in order, from most severe to least severe ones.
- **Aggd log level** - Specifies the log level for Aggd. The drop-down menu lists log levels in order, from most severe to least severe ones.
- **BGPd log level** - Specifies the log level for BGPd. The drop-down menu lists log levels in order, from most severe to least severe ones.
- **Alertd log level** - Specifies the log level for Alertd. The drop-down menu lists log levels in order, from most severe to least severe ones.
- **Pushd log level** - Specifies the log level for Pushd. The drop-down menu lists log levels in order, from most severe to least severe ones.
- **SNMPd log level** - Specifies the log level for SNMPd. The drop-down menu lists log levels in order, from most severe to least severe ones
- **NAPId log level** - Specifies the log level for NAPId. The drop-down menu lists log levels in order, from most severe to least severe ones

### STATS:

- **Collector data1 granularity (minutes)** - Specifies the aggregation granularity for data stored in flows1 table
- **Collector data2 granularity (minutes)** - Specifies the aggregation granularity for data stored in flows2 table
- **Collector data3 granularity (minutes)** - Specifies the aggregation granularity for data stored in flows3 table
- **Collector data1 keep time (minutes)** - Specifies the time for which to keep data in flows1 table
- **Collector data2 keep time (minutes)** - Specifies the time for which to keep data in flows2 table
- **Collector data3 keep time (minutes)** - Specifies the time for which to keep data in flows3 table
- **BGP data keep time (days)** - Specifies the time to keep data in the BGP table (used for BGP Report).

**Note:** Keep times indicated must be divisible between the tables.

### RESET DEFAULTS:

- **Changes all settings back to the default values.**

### REPORT CACHE:

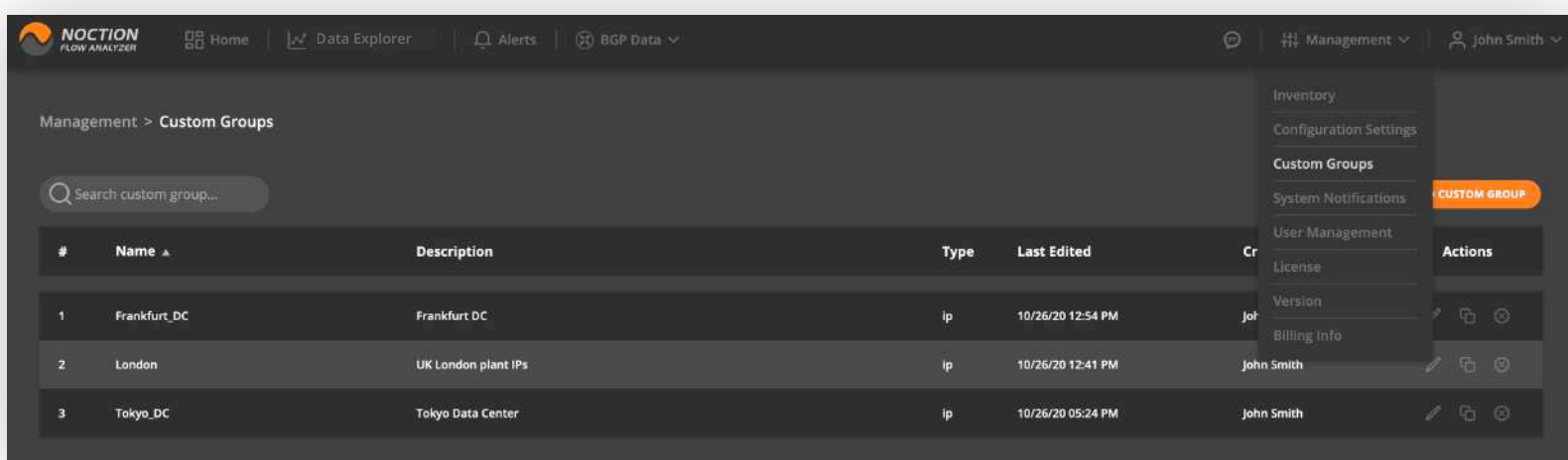
- **Query caching** - Enables/disables caching of the query results
- **Cached query lifetime (minutes)** - Specifies the lifetime of the cached query
- **Query cache max size (megabytes)** - Specifies the maximum cache size

**SNMP:**

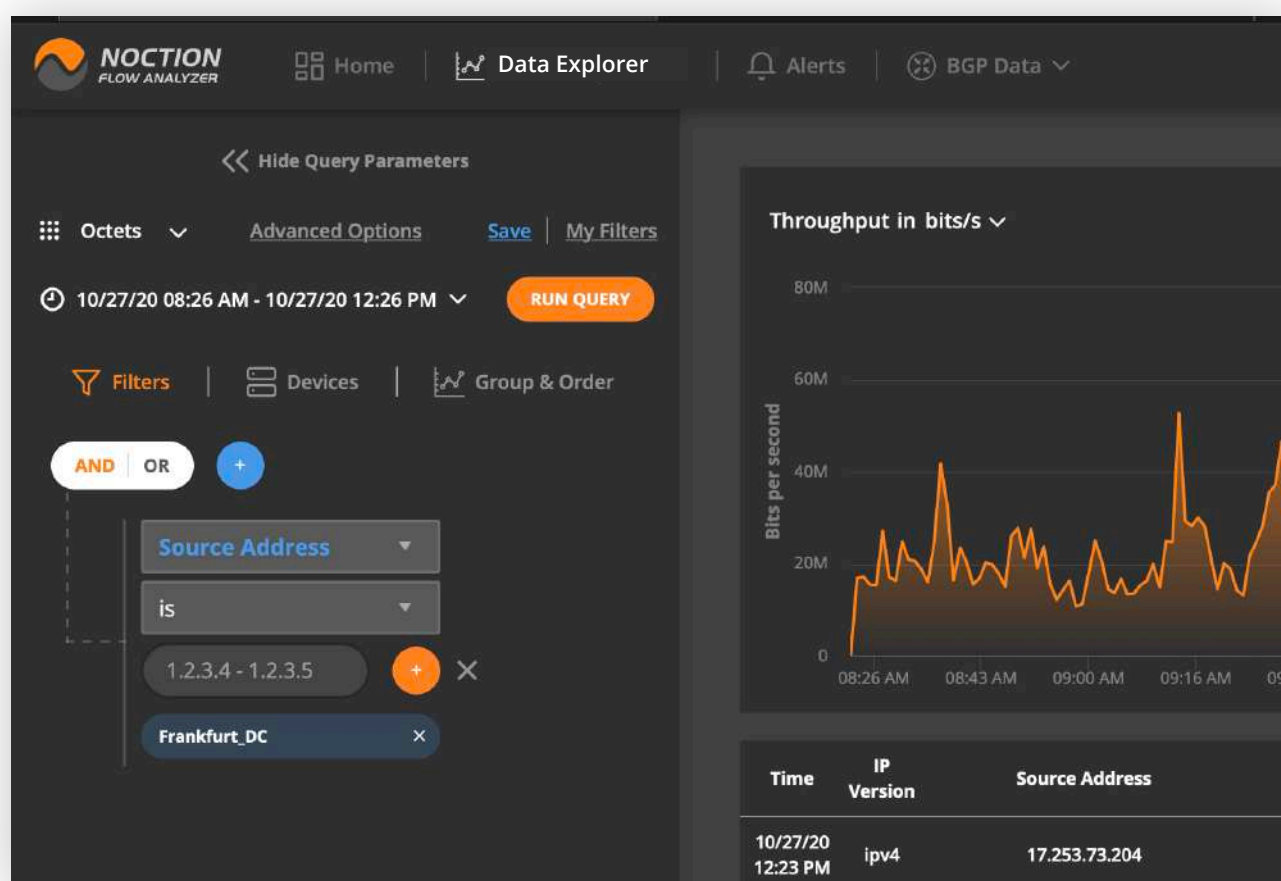
- **Time between successive interface info requests (seconds)** - The time interval between requests for the available interface details sent out by NFA.
- **SNMP requests timeout (seconds)** - The time interval that NFA waits for a response message from an agent. Increase the SNMP timeout value if there is higher latency in your network.
- **Number of retries before failing a request** - If a response from an SNMP Agent is not received before the timeout, then NFA retries the request the indicated number of times before reporting a failure.
- **Maximum number of repetitions for GetBulk request** - value for max repetitions field in the GETBULK PDU

### 3.3 Custom Groups

**Custom Groups** allow you to streamline and logically organize your network analysis experience by creating unique sets of data parameters to personalize your view in many areas of the Noction Flow Analyzer. For instance, you can create custom IP groups for your company’s specific departments, various geographic locations, or any other administrative/business requirement.



Once created, these can be used as custom filters when running queries in Data Explorer, creating widgets, setting up alerts, etc.

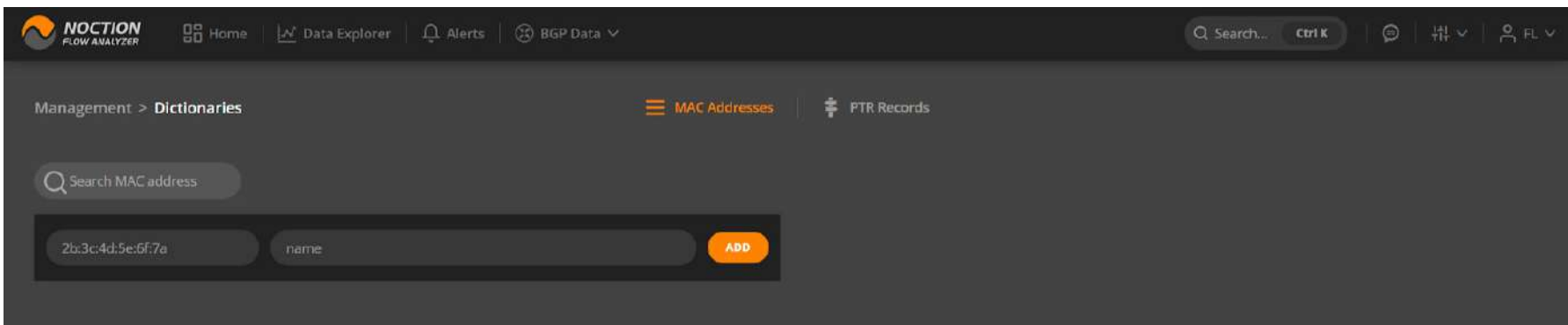




## 3.4 DICTIONARIES

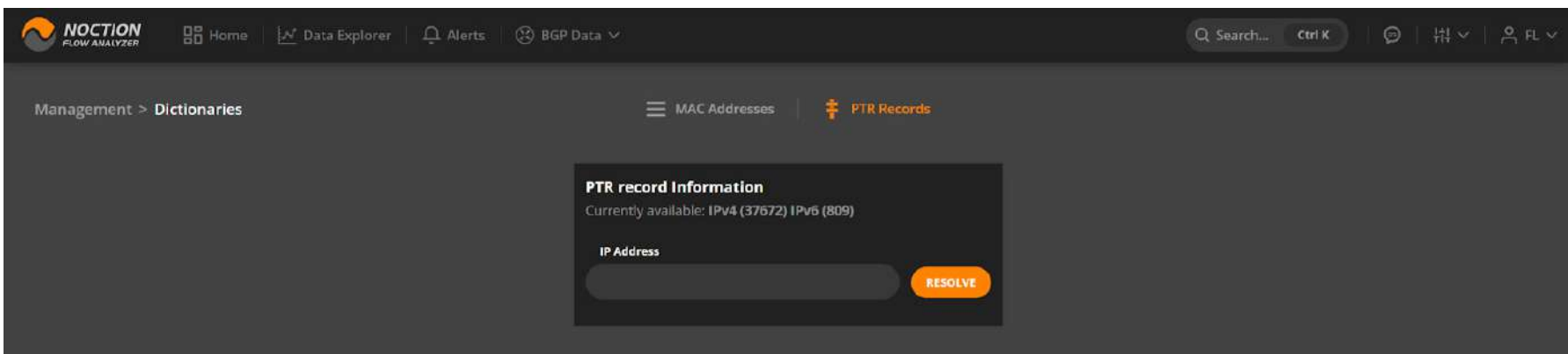
### 3.4.1 MAC Addresses

Go to **Management > Dictionaries > MAC addresses** to assign specific names to the MAC address records of interest. Whether you're tracking device connections, identifying anomalies, or enhancing your security protocols, the availability of a MAC address dictionary can streamline the completion of your recurrent network analysis and reporting tasks.



### 3.4.2 PTR Records

Go to the **PTR Records** tab under **Management > Dictionaries** to resolve IP addresses for specially crafted domain names. The result of the lookup is either a domain name that represents the reverse symbolic name or nothing (empty response).



## 3.5 SYSTEM NOTIFICATIONS

### 3.5.1 System Notifications Overview

System notifications are used to communicate to users the state of their NFA instance and/or any of its components. They are triggered by a range of preconfigured system-level events.

The list of events that can generate notifications is provided below.

Once an NFA component is started, stopped or reconfigured it raises the following events:

- Component Start: **OK**
- Component Start: **Error**
- Component Stop: **OK**
- Component Stop: **Error**
- Component Reconfig: **OK**
- Component Reconfig: **Error**
- Config Validation: **OK**
- Config Validation: **Error**

BGPd raises the following events when BGP sessions are established/disconnected:

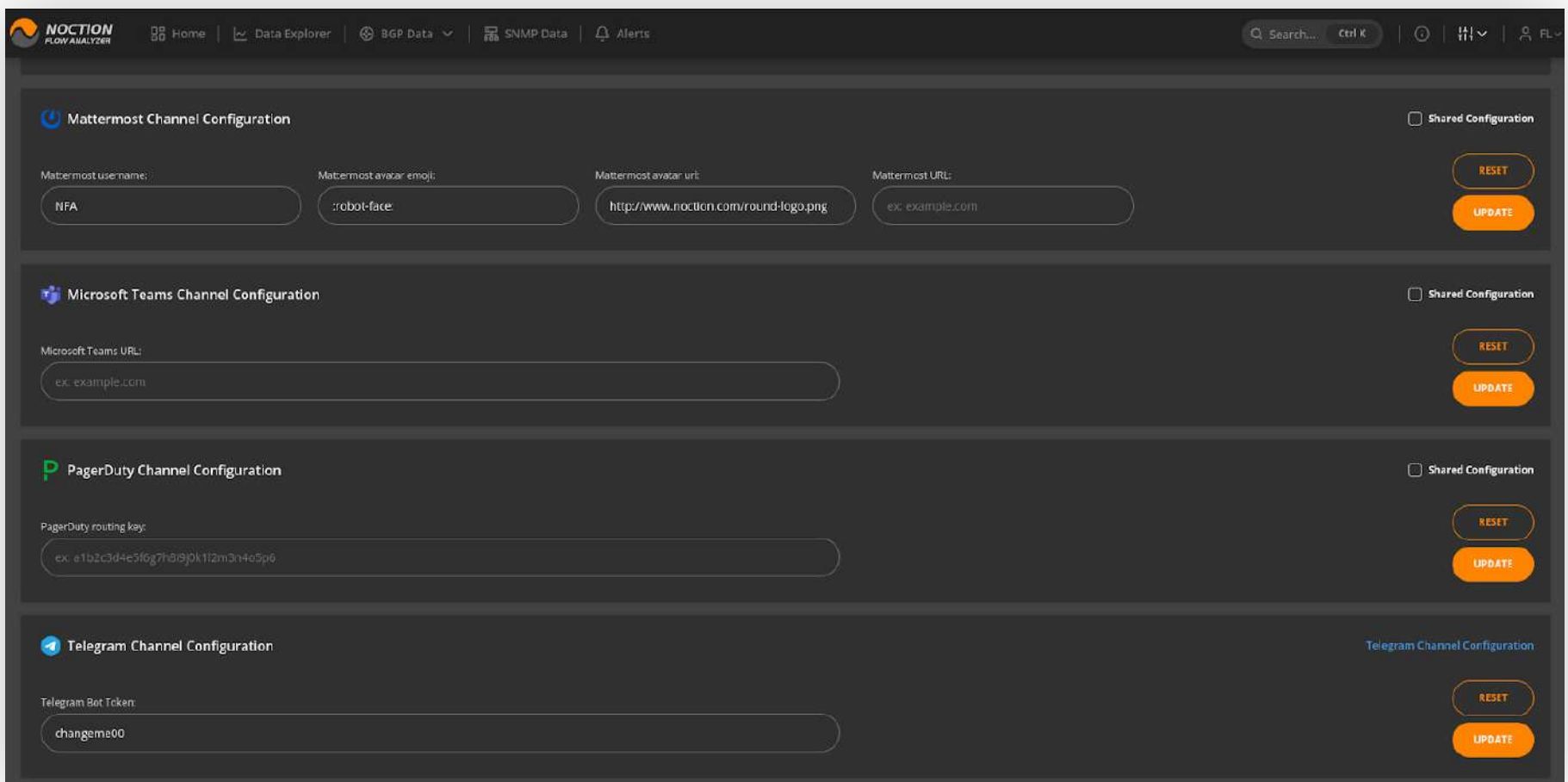
- NFA BGP session **disconnected**
- NFA BGP session **established**

FLOWd raises the following events when Flow Stream is Started/Stopped:

- Flow Stream **Start**
- Flow Stream **Stop**

### 3.5.2 System Notification Channels Configuration

In order for notifications to be delivered correctly, the corresponding Email, Telegram, Mattermost, or Slack channel configuration shall be provided. Go to **Management > System Notifications > Notification Channels**.



The screenshot shows the 'Notification Channels' configuration page in the Noction Flow Analyzer. The page is dark-themed and contains four configuration sections, each with a 'Shared Configuration' checkbox in the top right corner. The sections are:

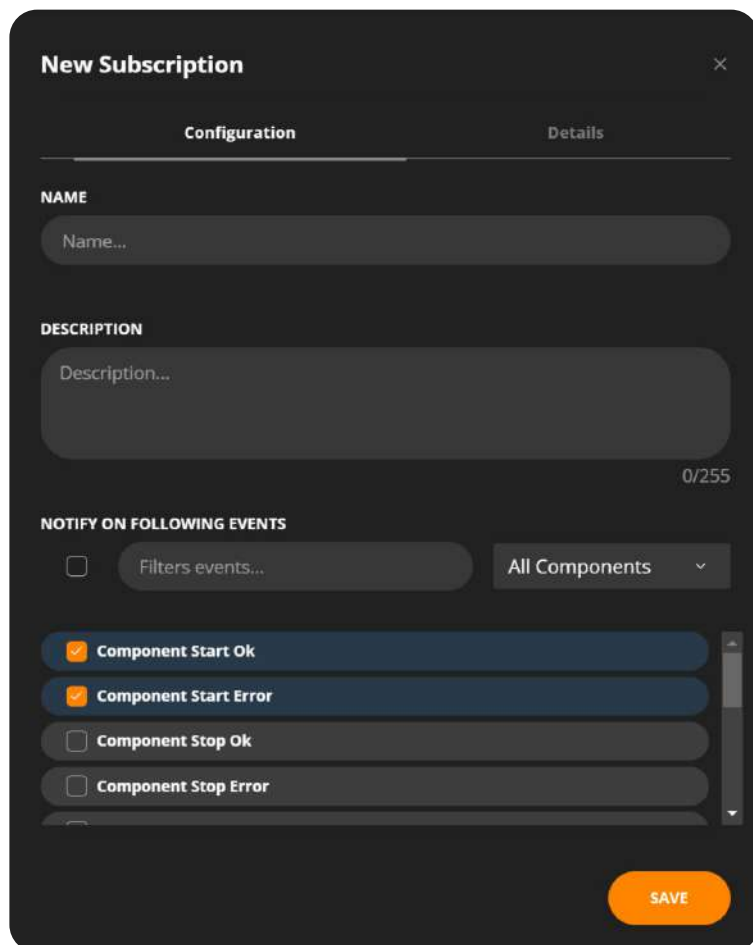
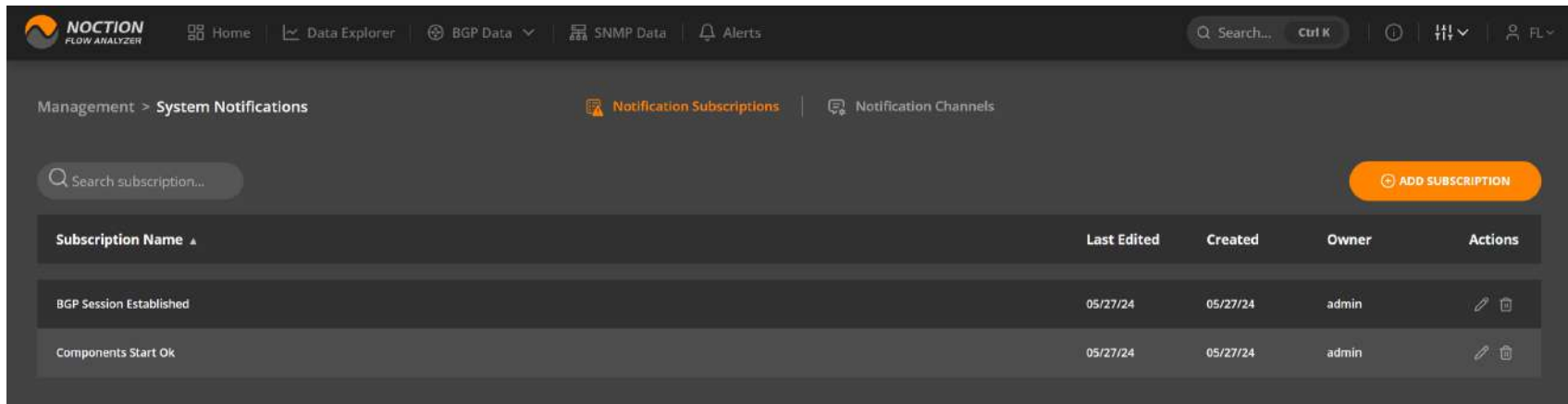
- Mattermost Channel Configuration:** Includes input fields for 'Mattermost username' (NFA), 'Mattermost avatar emoji' (:robot-face), 'Mattermost avatar url' (http://www.noction.com/round-logo.png), and 'Mattermost URL' (ex: example.com). Buttons for 'RESET' and 'UPDATE' are on the right.
- Microsoft Teams Channel Configuration:** Includes an input field for 'Microsoft Teams URL' (ex: example.com). Buttons for 'RESET' and 'UPDATE' are on the right.
- PagerDuty Channel Configuration:** Includes an input field for 'PagerDuty routing key' (ex: a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6). Buttons for 'RESET' and 'UPDATE' are on the right.
- Telegram Channel Configuration:** Includes an input field for 'Telegram Bot Token' (changema00). Buttons for 'RESET' and 'UPDATE' are on the right.

For the email channel configuration, specify the actual Email server and Server port as well as the sender of email messages that will show in the receiver's inbox. Optionally, select encryption and set a password. For the Slack, Microsoft Teams, and Mattermost channels configuration, specify the bot name and/or URL. For Telegram, provide the proper bot token. For the PagerDuty Channel Configuration, provide the routing key.

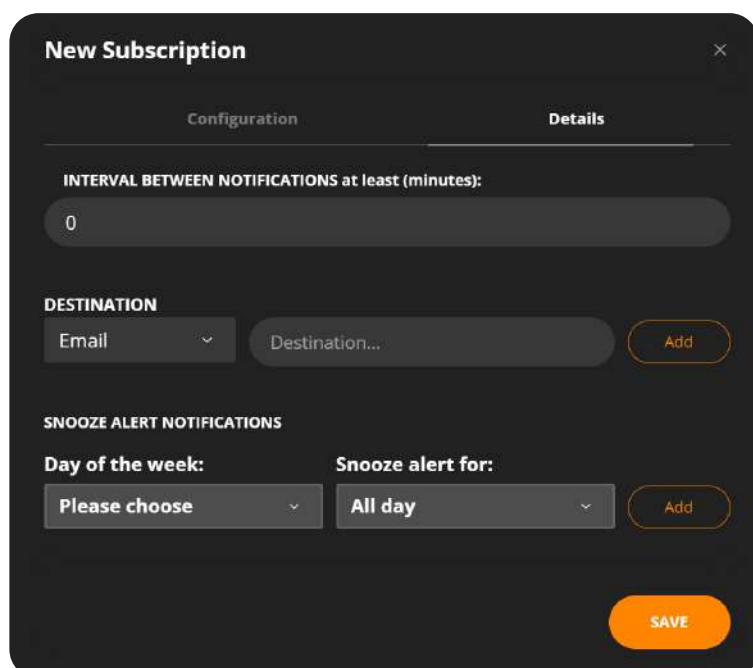
### 3.5.3 System Notification Subscriptions

System Notifications are sent only if a valid subscription to events has been created.

Find the list of your active subscriptions under **Management > System Notifications > Notification Subscriptions**. Search through existing subscriptions, sort, view, edit, or delete them.



To create a new subscription click the “**Create New Subscription**” button in the top right corner. A popup window will appear. Under the “**Configuration**” tab, provide your subscription topic and description. Choose the proper group or use the quick search option to find and checkmark the desired event(s). Hit “**Save**”.



Now, under the “**Details**” tab, introduce the “Interval between notifications” as well as the destination email or Slack channel. Optionally, specify when to Snooze Notifications if desired and hit “**Save**”.

### 3.5.4 Notification Text Details

When a subscribed event is fired NFA will send notifications. The notification email will consist of the following:

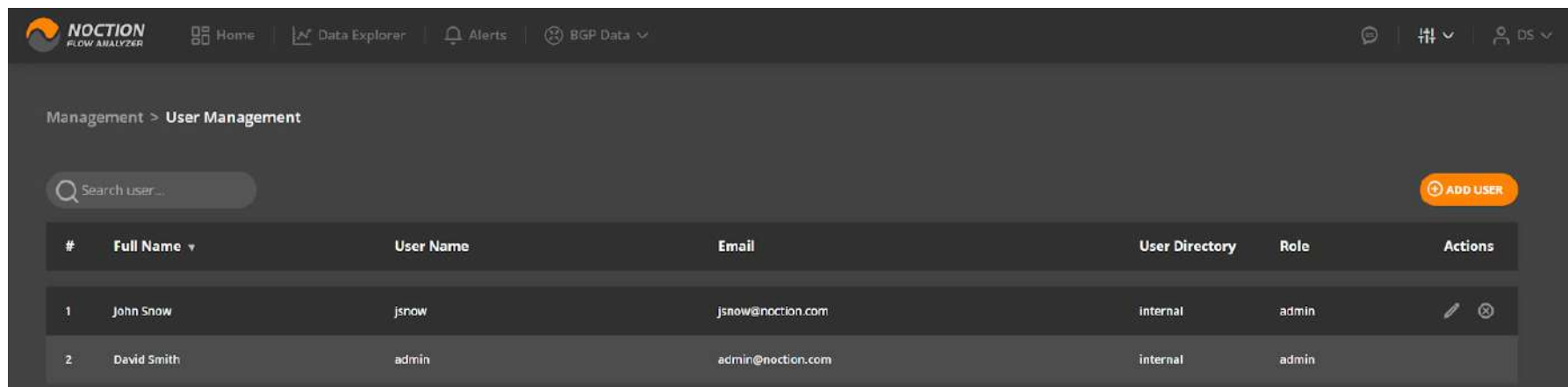
1. Subscription topic as specified in the subscription
2. From email address - as configured in the email channel
3. Time - date-time of the last event that caused the notification. In case of rate limitation, this might be older than the time of the email.
4. Textual description of the event and any related details.
5. Older events which have been retained due to rate limitations. Keep in mind that all past events are aggregated into a single email.

## 3.6 User Management and User Directories

### 3.6.1 User Management

NFA includes a User Management function accessible under Management main menu section, that allows the following:

- review and filter the list of users
- edit and delete existing user records
- add new users



### 3.6.2 LDAP User Directories

LDAP user directories can be added, updated and removed from NFA by accessing **Management > User Management**. Each user directory takes a series of parameters specific for the protocol.

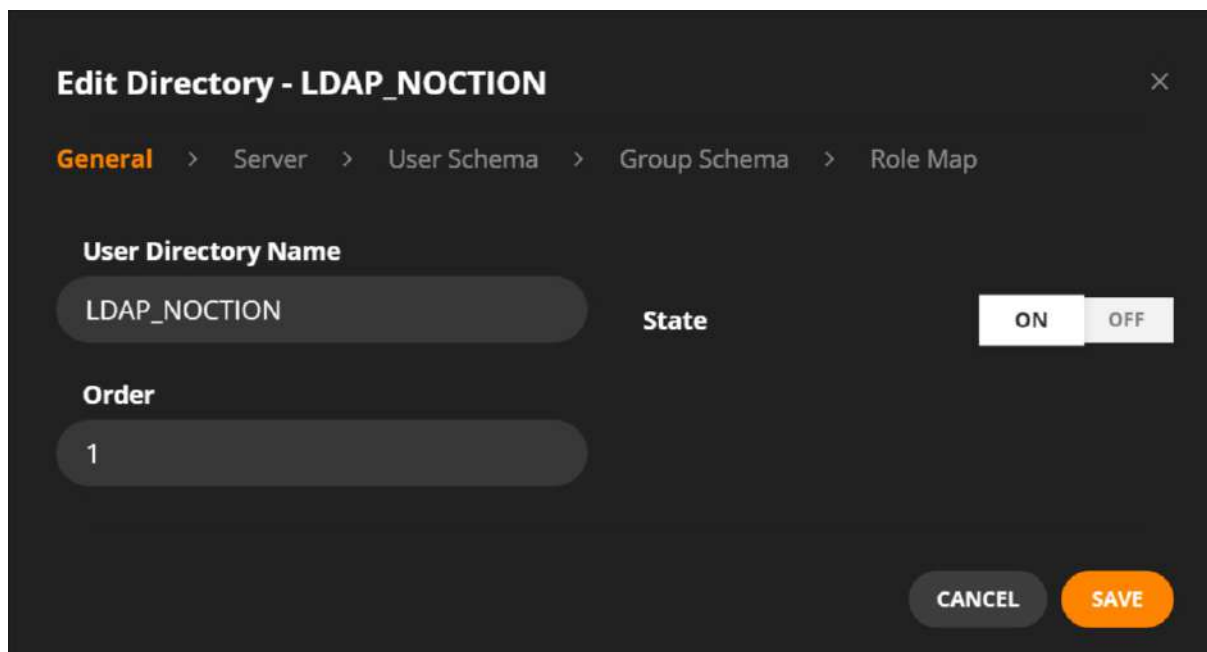
**Note:** All operations with DNs (initial bind DN, group DNs, user names) are case insensitive and also strip redundant whitespace.

Refer to individual protocol documentation for how to correctly configure one or another user directory.

The example below offers a generic set of parameters required to configure NFA to use Active Directory for access management.

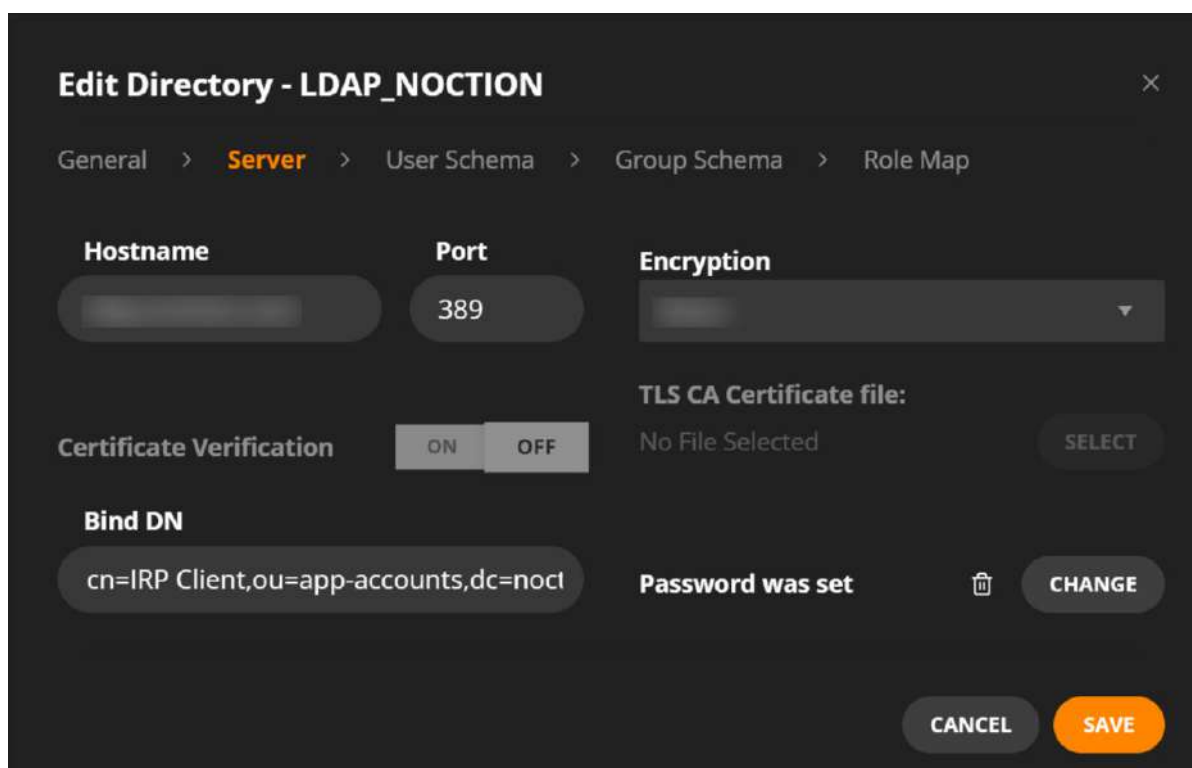
The general tab covers:

- User directory name - the name assigned to the directory within NFA
- User directory type
- State - a toggle to enable or disable a user directory,
- Order specifies when this user directory will be examined by NFA compared to other user directories



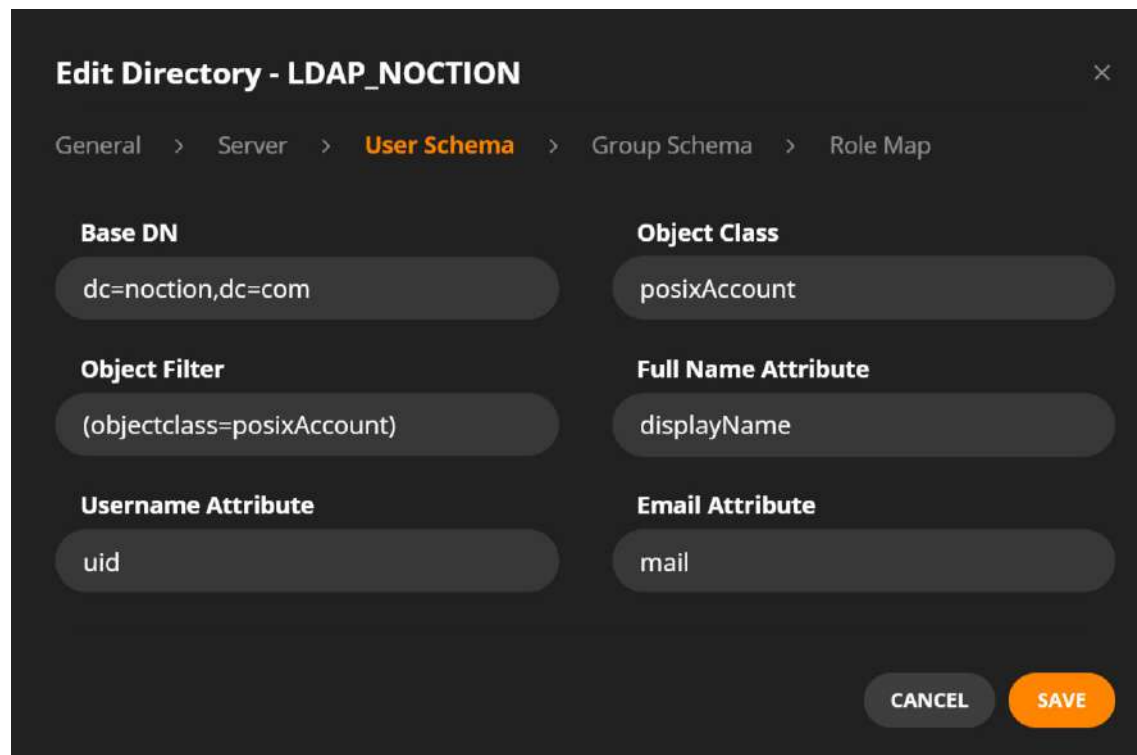
The server tab covers:

- User directory hostname in the form of either IP address or domain name (LDAP/LDAPS)
- User directory port
- SSL, TLS, or no encryption selector
- Certificate verification toggle and TLS CA Certificate file options in case the TLS encryption is selected
- The binding user name that NFA uses to authenticate itself
- Bind password assigned to NFA



The user schema tab covers:

- The Generic, LDAP POSIX, or Active Directory type selector
- Base DN specifies the root distinguished name and user subtree
- Object Class - an attribute that defines the characteristics of an object in the directory
- Object Filter - a search criterion used to find objects in the directory that match a specific set of attributes
- Username, Email, and Full Name fields map the User Directory attributes to NFA user attributes

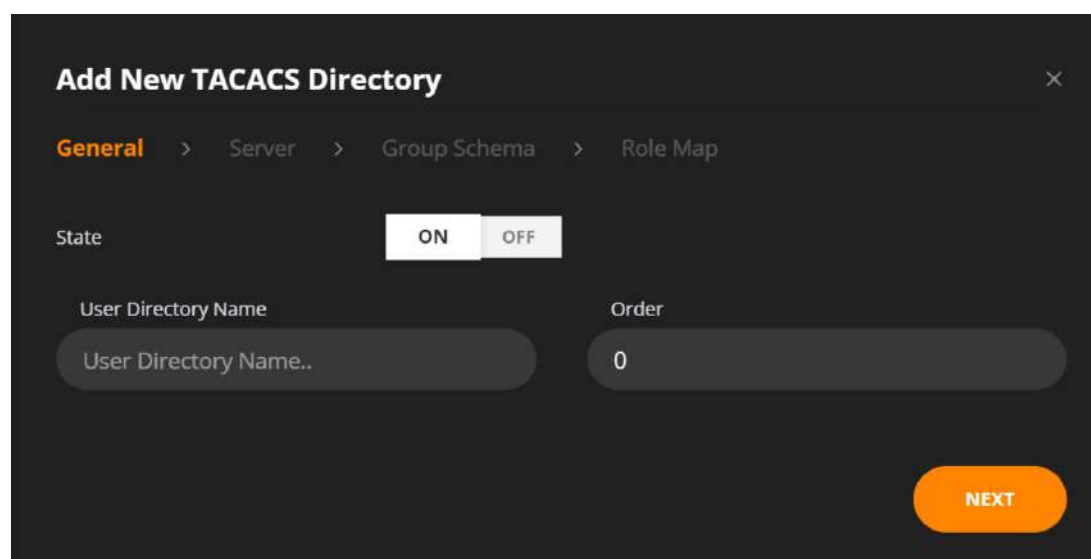


### 3.6.3 TACACS+ user directories

TACACS+ user directories can be added, updated and removed from NFA by accessing **Management > User Management**. User directory takes a series of parameters specific for the protocol.

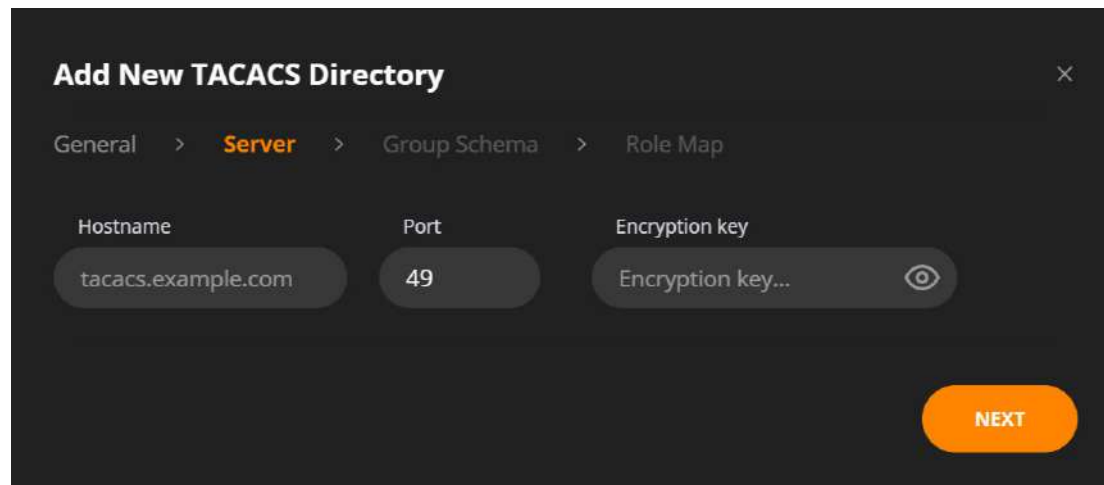
The general tab covers:

- User directory name - the name assigned to the directory within NFA
- State - a toggle to enable or disable a user directory,
- Order specifies when this user directory will be examined by NFA compared to other user directories



The server tab covers:

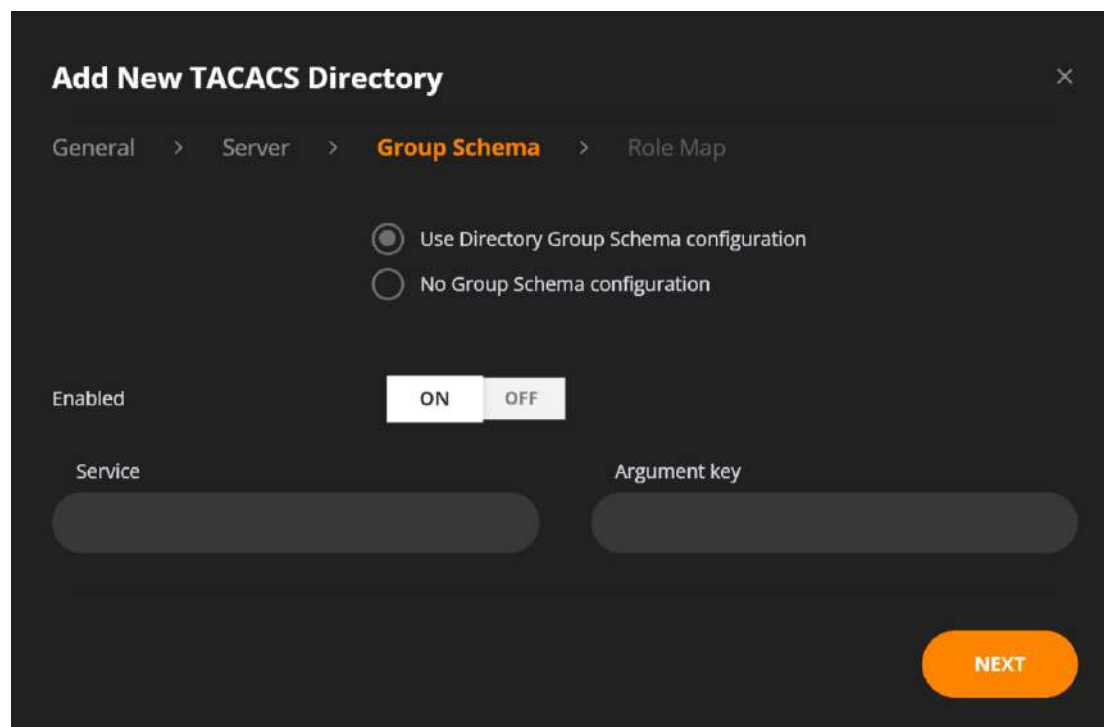
- User directory hostname in the form of either IP address or domain name
- User directory port
- Encryption key



The screenshot shows the 'Add New TACACS Directory' dialog with the 'Server' tab selected. The breadcrumb navigation is 'General > Server > Group Schema > Role Map'. There are three input fields: 'Hostname' with the value 'tacacs.example.com', 'Port' with the value '49', and 'Encryption key' with a placeholder 'Encryption key...' and a toggle icon. An orange 'NEXT' button is at the bottom right.

The group schema tab covers:

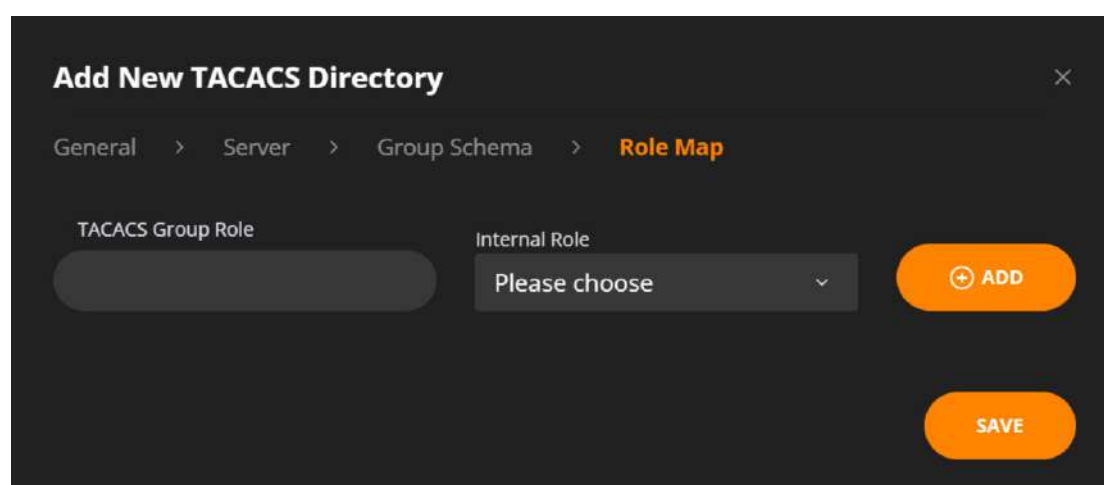
- The Service parameter
- The Argument Key



The screenshot shows the 'Add New TACACS Directory' dialog with the 'Group Schema' tab selected. The breadcrumb navigation is 'General > Server > Group Schema > Role Map'. There are two radio buttons: 'Use Directory Group Schema configuration' (selected) and 'No Group Schema configuration'. Below them is an 'Enabled' toggle switch set to 'ON'. There are two input fields: 'Service' and 'Argument key'. An orange 'NEXT' button is at the bottom right.

The role map tab covers:

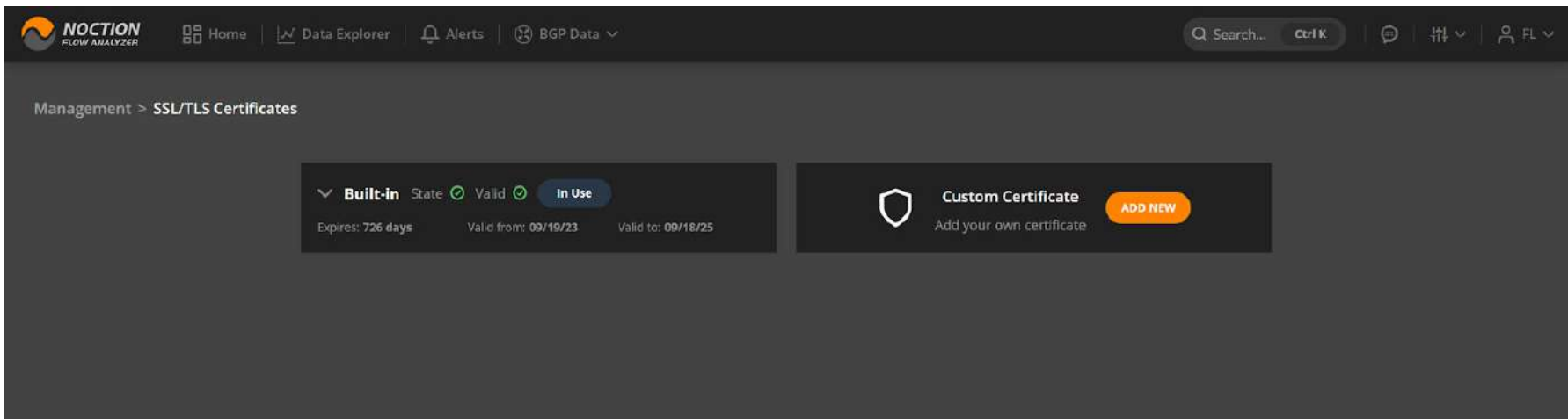
- TACACS Group Role
- Internal NFA role (Admin / User)



The screenshot shows the 'Add New TACACS Directory' dialog with the 'Role Map' tab selected. The breadcrumb navigation is 'General > Server > Group Schema > Role Map'. There are two input fields: 'TACACS Group Role' and 'Internal Role' with a dropdown menu showing 'Please choose'. There are two orange buttons: 'ADD' and 'SAVE'.

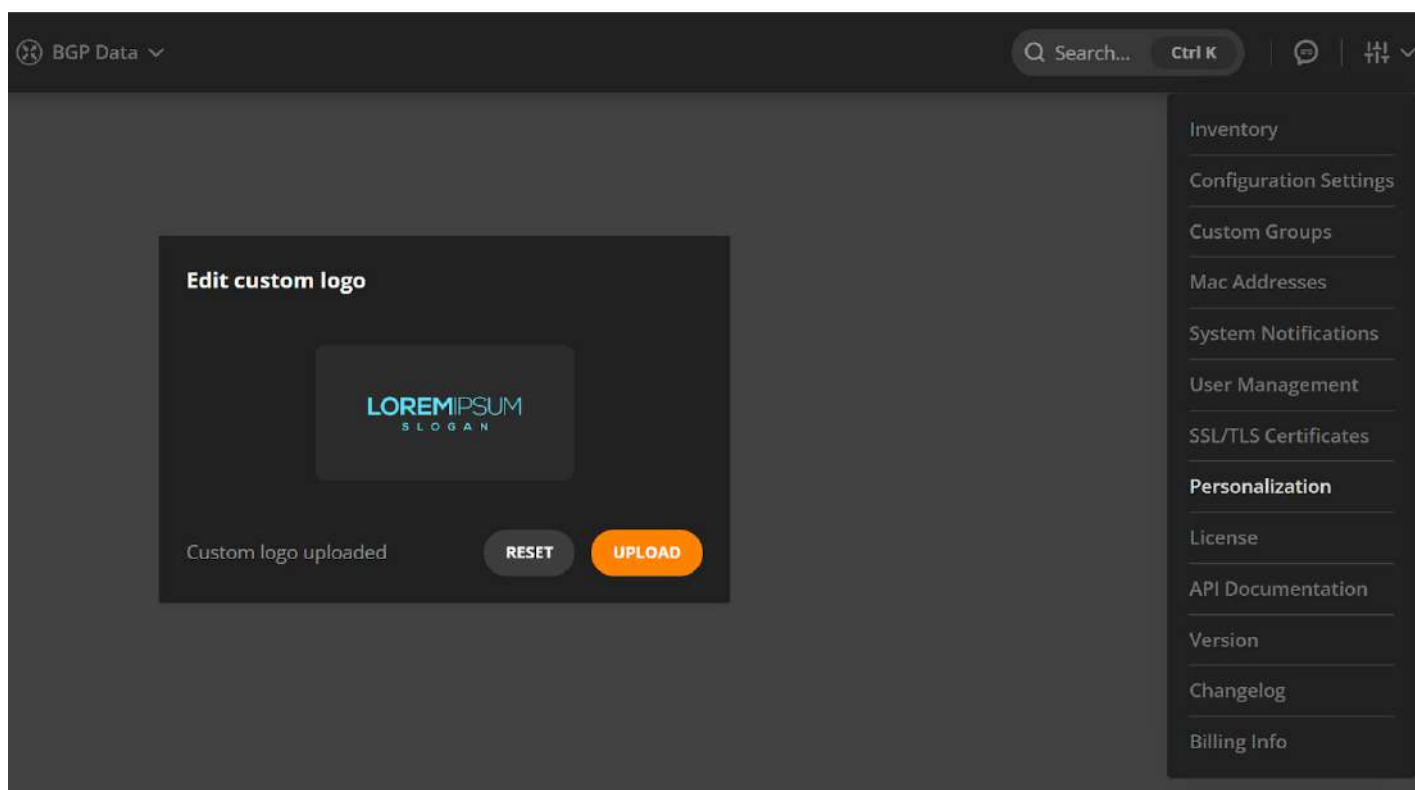
### 3.7 SSL/TLS Certificates

NFA uses a built-in certificate by default. To choose and apply a custom certificate that aligns with your security policies, go to **Management > SSL/TLS certificates** and click the **ADD NEW** button in the corresponding section. Introduce the certificate body, an optional chain, as well as the private key, and hit **SUBMIT**.



### 3.8 Personalization

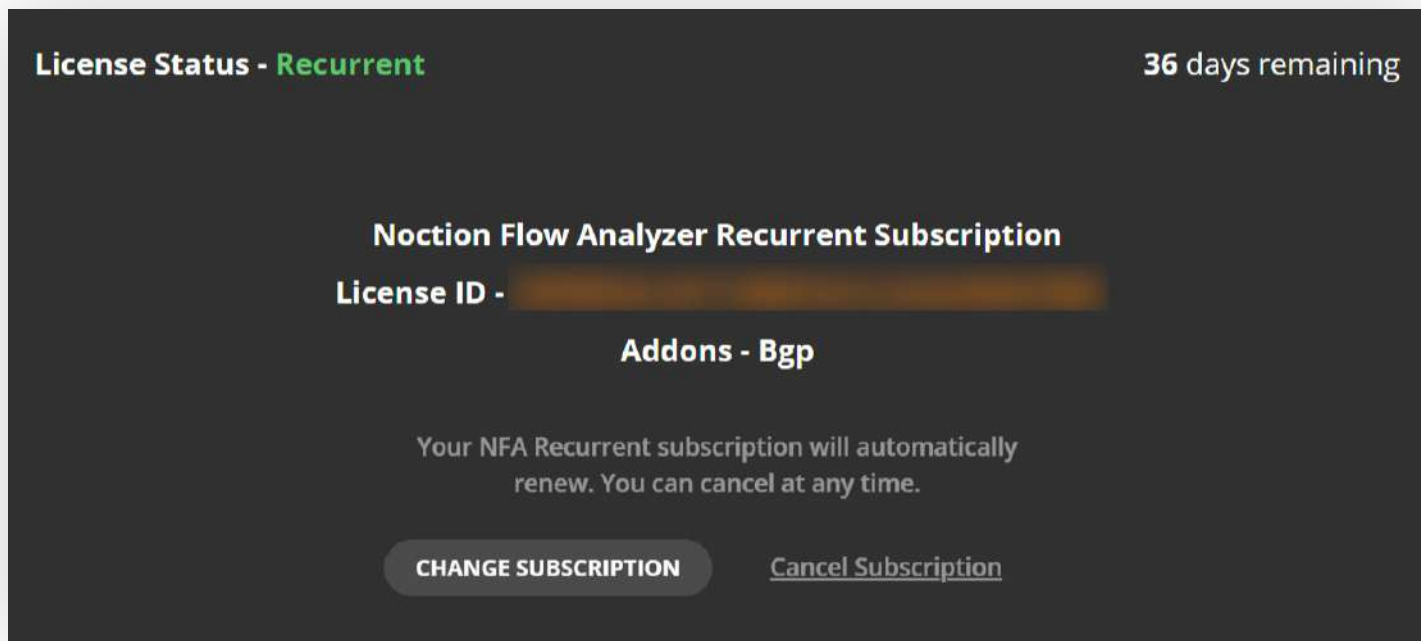
Go to **Management > Personalization** and upload a custom logo for a personalized touch to your NFA interface.





### 3.9 License Status

NFA is a licensed product and requires users to obtain and register their license in the application. The license status is accessed by navigating to **Management > License**.



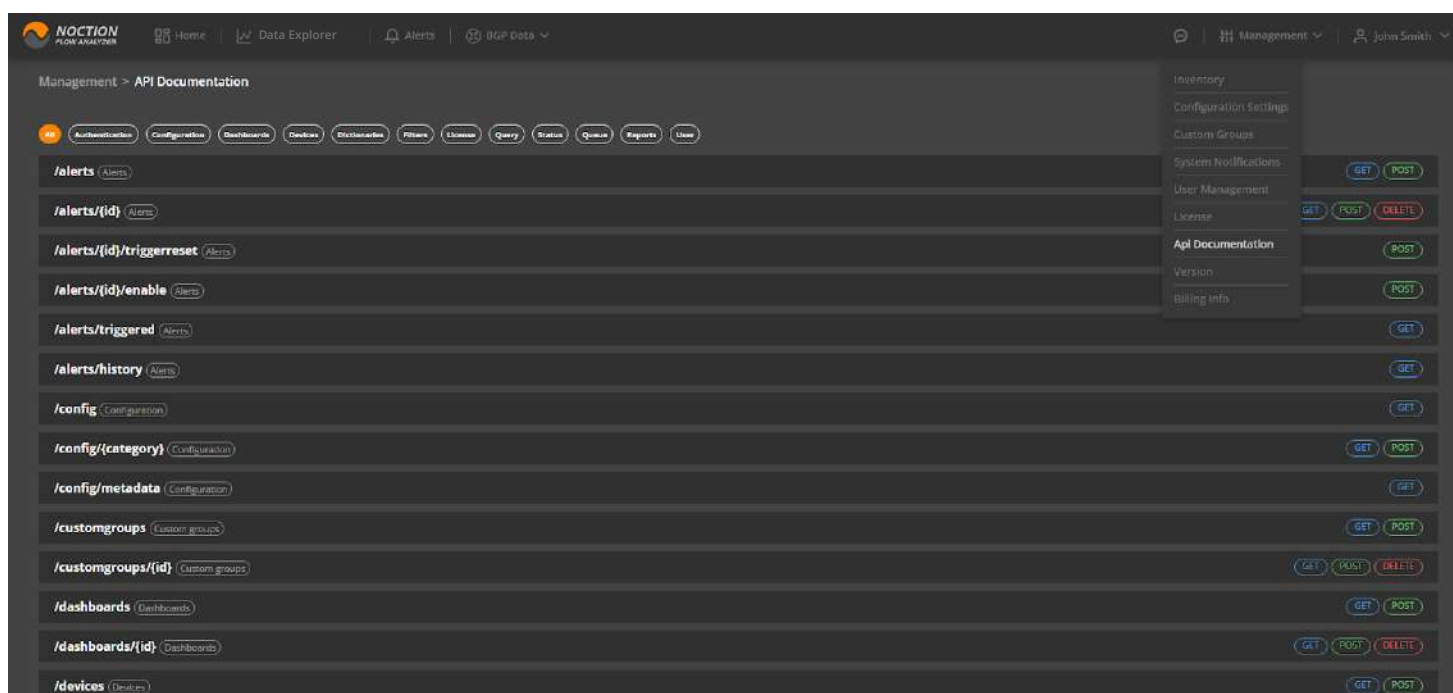
License status offers:

- information about current license status and the remaining days till its expiration
- option to activate a license by means of an activation key
- information about the current license & add-on status and the remaining days till expiration

**PURCHASE LICENSE** redirects users to Noction’s billing system to place an order for a license.

### 3.10 API Documentation

Noction Flow Analyzer API provides a wide range of capabilities to access NFA data. It lets users read all the resources including dashboards, widgets, devices, alerts, filters, reports, and more. Some of these resources are read-only and some can also be created/edited/deleted via the API. The API documentation is available via the NFA’s frontend under the **Management > API Documentation** section.

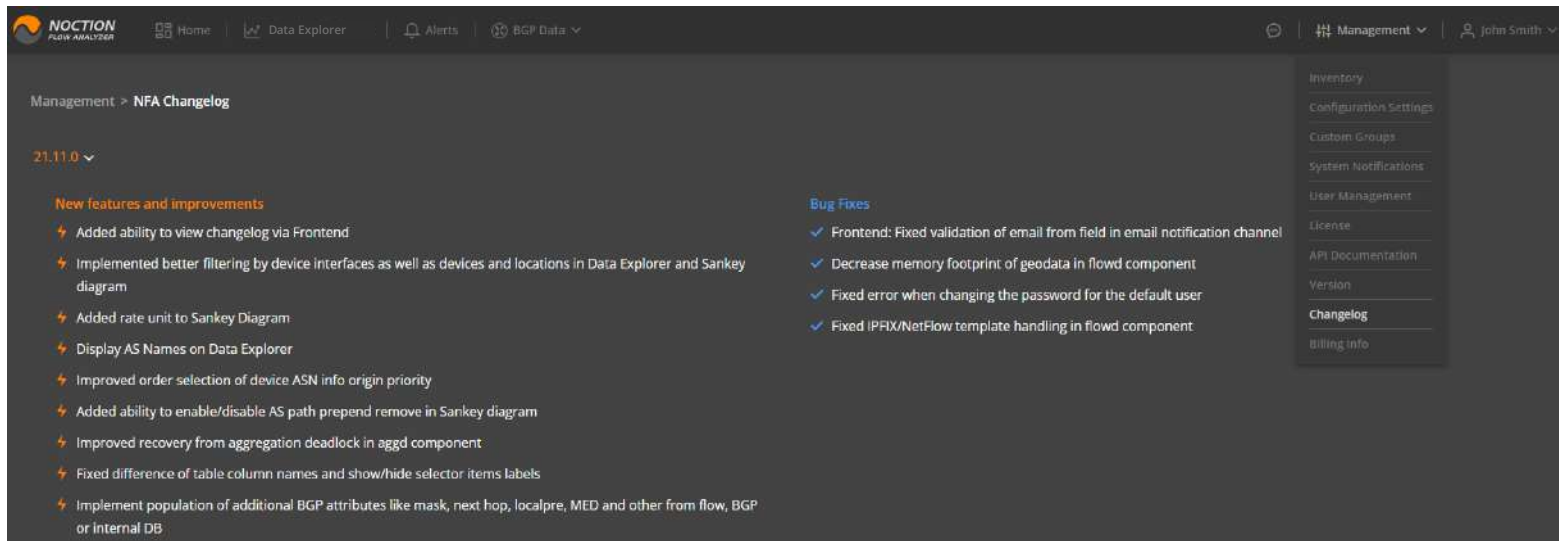


### 3.11 NFA Version

NFA Version info is available to be able to manage the change and configuration of the application.

### 3.12 Changelog

The Changelog section is available under **Management > Changelog**. It offers a complete list of improvements and bug fixes per each NFA version.



### 3.13 Billing Info

To access your billing info, go to **Management > Billing**. The link will redirect you to the NFA Billing page. Use the credentials you've specified when initially requesting an NFA license to login.

## 4. User Profile, Requirements and Support

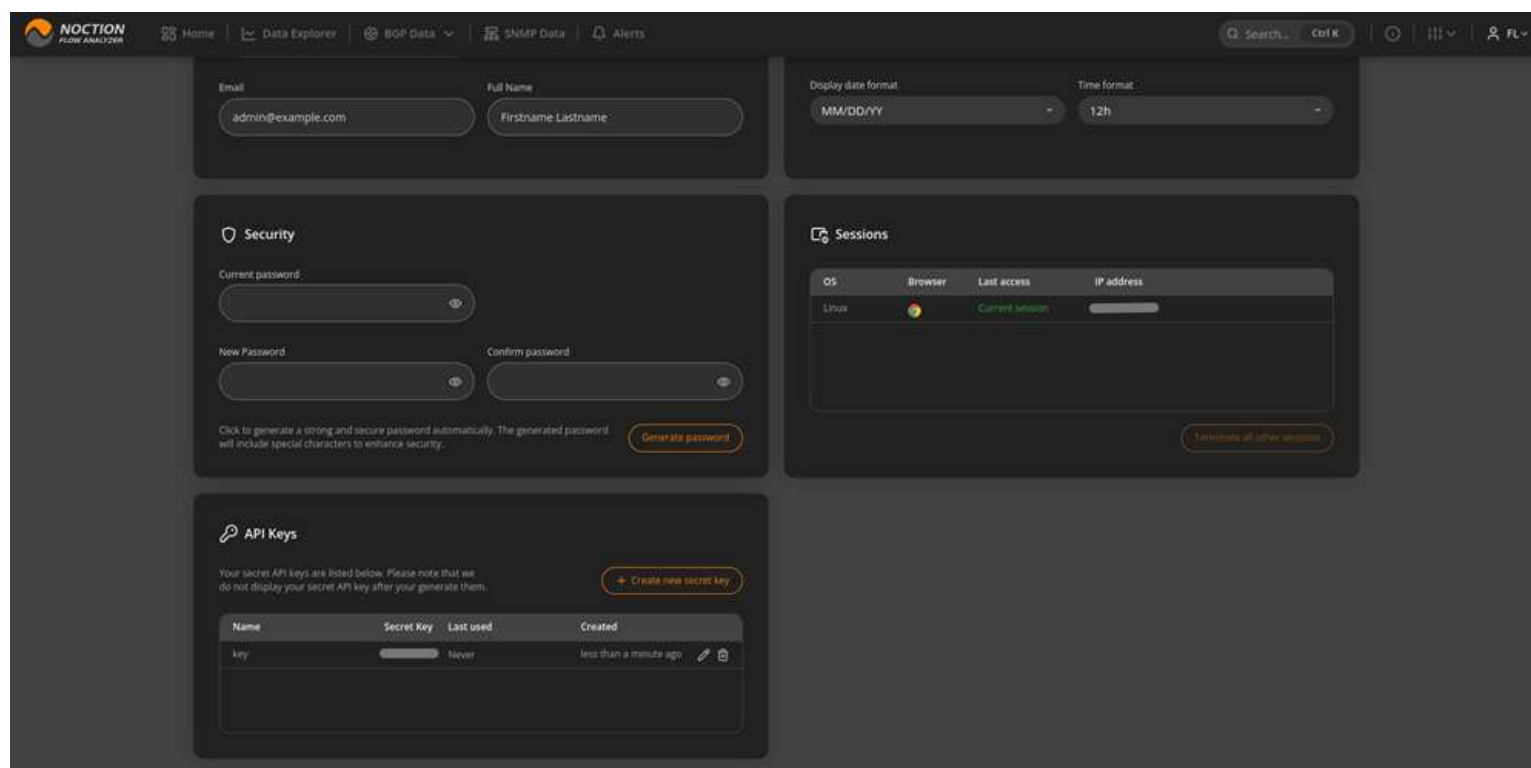
### 4.1 User Profile

The user profile helps in associating characteristics with a specific user and helps to ascertain the interactive behavior of the user along with preferences.

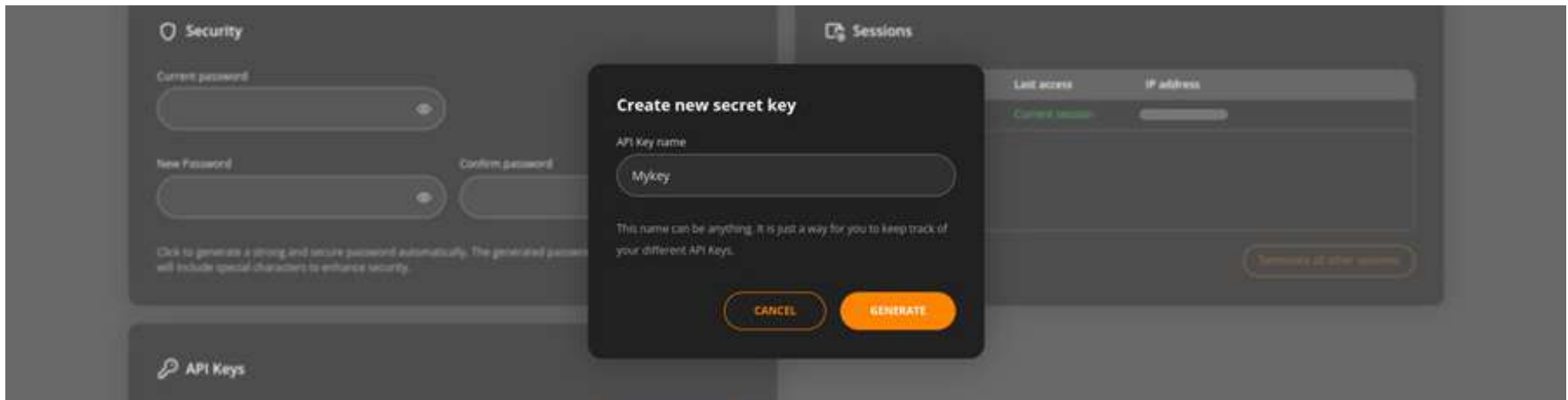
Users with administrative rights have access to and can edit any user profile. Users without admin rights have access to and can edit their user profile only.

The Profile page is thoughtfully organized into four distinct sections: Account, Personalization, Security, and Sessions.

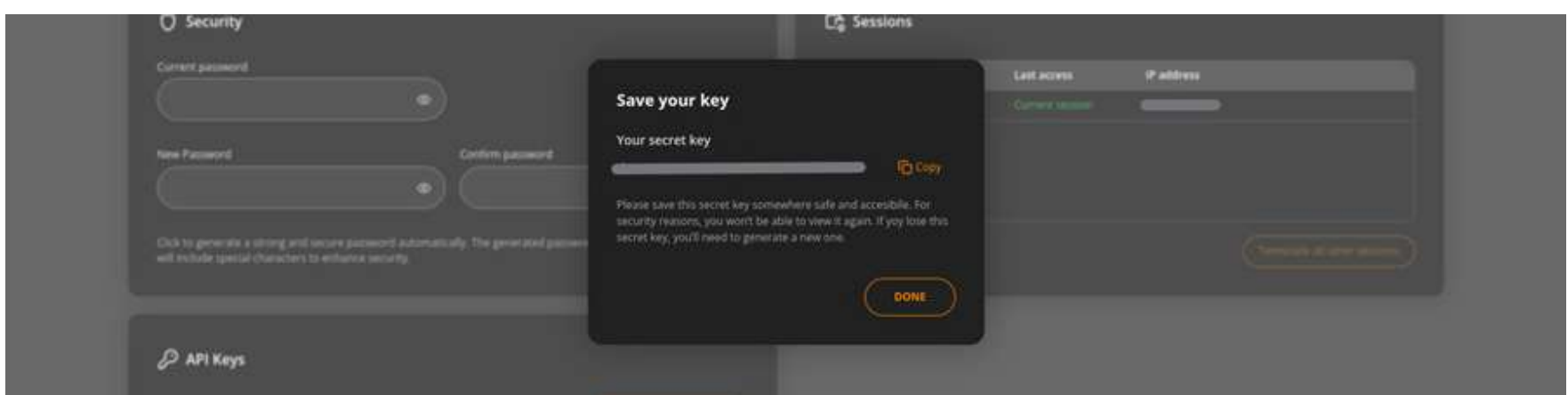
- **Account:** This section displays essential details such as your **Username, Email, and Full Name**. For internal users, there is the flexibility to update both the **Email** and **Full Name**.
- **Personalization:** Here, you can tailor your user experience by selecting your preferred **Interface theme** — with options like **Auto, Dark, and Light**. Additionally, you have the ability to customize the **Date and Time format** to suit your preferences.
- **Security:** In this section, you can enhance your account’s security by updating your password. Simply enter your current password, then input your desired new password. If you prefer, you can also opt for the system to generate a secure password automatically by clicking on “Generate password.”
- **Sessions:** This section provides a comprehensive overview of all your active sessions, displaying details such as **Operating System (OS), Browser, and IP Address**. You have the option to terminate any session or end all sessions with a single click—except for your current session, which remains protected from termination.
- **Browser Notifications:** Enable browser notifications to receive real-time updates and notifications even when you’re away from NFA. Browser notifications are different from the mandatory in-app notifications, which are enabled by default.
- **API Keys:** An API key is a unique identifier used to authenticate a user making requests to an API. This approach offers a major advantage: it enables seamless integration with other applications. Different systems can communicate securely using API keys, allowing one application to access NFA services or data without needing a user login.



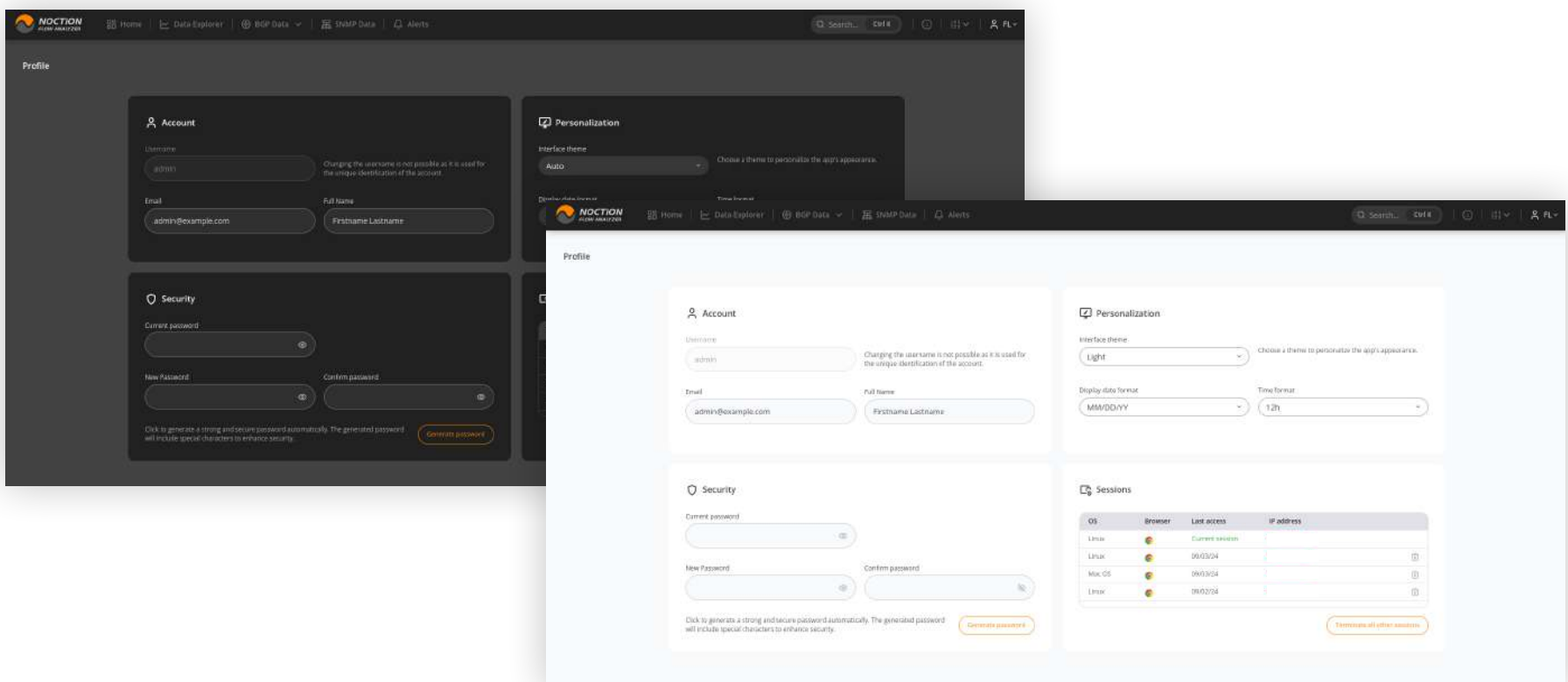
By clicking “Create new secret key,” you will need to specify the name of the API key.



Once the API key is generated, store it in a safe and accessible location. For security reasons, you won't be able to view it again. The list of API keys will be displayed in the API Keys section, where you can edit the name of any key or delete specific keys as needed.



The image below showcases the interface in its Dark & Light themes.



## 4.2 System Requirements

### Hardware Requirements:

- x86\_64 architecture
- Minimum 4x core CPU (8x core CPU recommended), SSE4.2 support
- Minimum 32GB of RAM (64GB RAM recommended; 128GB RAM - optimal)
- Minimum 250GB SSD storage (500GB SSD storage recommended) allocated to the /var partition

### Software Requirements:

- Ubuntu 22.04, Ubuntu 22.04 or Ubuntu 24.04 LTS

Please note that NFA can also be installed on a server running RHEL 8 / RHEL 9. The minimum system requirements assume default configuration. Significantly increasing the flow collection rate might cause additional load on a server, thus requiring extra memory or a larger CPU.

Hardware resources depend on the amount of flows/s exported to NFA. For each additional 1,000 flows/sec, 1 GB of RAM and 0.2 of vCPU are required. An additional 2 GB of RAM and 4 vCPU are required when the BGP add-on is used. Values are directly proportional: RAM and vCPU numbers per 1,000 flows/sec.

For instance: 40,000 flows/sec will require 40 GB of RAM and 8 vCPU, plus 2 GB of RAM and 4 vCPU in case a BGP add-on is used.

## 4.3 Support

Noction support team is available 24/7. Please contact our support team by emailing [support@noction.com](mailto:support@noction.com) or by calling +1 (650) 903-7028.

## 5. Flow export configuration on network devices

---

### Cisco XE:

The NetFlow infrastructure is based on the configuration and use of the following maps:

- Exporter Map
- Sampler Map
- Flow Monitor Map

1. Exporter Map. To configure the Exporter map, you need to define the destination (flow collector), the source interface, the port used for exporting, the version of NetFlow, and the timeout rates:

```
router(config)# flow exporter-map EM
router(config-fem)# destination 10.1.1.5
router(config-fem)# source gi0/0
router(config-fem)# transport udp 2055
router(config-fem)# version v9
router(config-fem)# template data timeout 60
router(config-fem)# options interface-table timeout 60
router(config-fem)# exit
```

## 2. Sampler Map (defines the sample rate):

```
router(config)# sampler-map SM
router(config-sm)# random 1 out-of 1000
router(config)# exit
```

## 3. Flow Monitor Map. The Flow Monitor map defines the cache timeout values and associates the exporter map with this map:

```
router(config)# flow monitor-map FMM
router(config-fmm)# record ipv4
router(config-fmm)# exporter EM
router(config-fmm)# cache timeout active 60
router(config-fmm)# cache timeout inactive 60
router(config-fmm)# exit
```

## 4. Apply the maps to the interfaces. Now that you have your maps defined, you need to apply the Flow Monitor and Sampler maps to each of the provider interfaces:

```
router(config)# interface Gi0/0
router(config-if)# flow ipv4 monitor FMM sampler SM egress
router(config-if)# exit
```

### Cisco XE:

```
flow exporter EXPORTER-1
 destination 172.16.10.2
 export-protocol netflow-v9
 transport udp 2055
 exit
!
flow record v4_r1
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect counter bytes long
 collect counter packets long
!
flow monitor FLOW-MONITOR-1
 record v4_r1
 exporter EXPORTER-1
!
interface GigabitEthernet 0/0/0
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 input
```

### Cisco IOS:

```
ip flow-export version 9
ip flow-export destination $NFA_IP 2055
interface $Interface_to_ISP1
 ip flow ingress
 ip flow egress
```

**jFlow-ipfix:**

```
chassis {
  fpc 0 {
    sampling-instance nfa-instance;
  }
}
interfaces {
  xe-0/0/0 {
    unit 0 {
      family inet {
        sampling {
          input;
          output;
        }
      }
    }
  }
}
forwarding-options {
  sampling {
    instance {
      inst1 {
        input {
          rate 1024;
        }
        family inet {
          output {
            flow-server X.X.X.X {
              port 2055;
              version-ipfix {
                template {
                  ipfix-templatev4;
                }
              }
            }
            inline-jflow {
              source-address Y.Y.Y.Y;
            }
          }
        }
      }
    }
  }
}
services {
  flow-monitoring {
    version-ipfix {
      template ipfix-templatev4 {
        flow-active-timeout 60;
        flow-inactive-timeout 60;
        template-refresh-rate {
          seconds 60;
        }
      }
    }
  }
}
```

```
        ipv4-template;
    }
}
}
```

X.X.X.X - IP address of NFA server

Y.Y.Y.Y - source IP address of flow packets (router IP address)

### jFlow-v9:

```
chassis {
    fpc 0 {
        sampling-instance nfa-instance;
    }
}
interfaces {
    xe-0/0/0 {
        unit 0 {
            family inet {
                sampling {
                    input;
                    output;
                }
            }
        }
    }
}
forwarding-options {
    sampling {
        instance {
            nfa-instance {
                input {
                    rate 1024;
                }
                family inet {
                    output {
                        flow-server X.X.X.X {
                            port 2055;
                            version9 {
                                template {
                                    v9-templatev4;
                                }
                            }
                        }
                    }
                }
            }
        }
    }
}
services {
    flow-monitoring {
        version9 {
```



```
        template v9-templatev4 {
            flow-active-timeout 60;
            flow-inactive-timeout 60;
            template-refresh-rate {
                seconds 60;
            }
            ipv4-template;
        }
    }
}
```

X.X.X.X - IP address of NFA server

Y.Y.Y.Y - source IP address of flow packets (router IP address)

### sFLOW-Arista:

```
!
sflow run
sflow source $SOURCE
sflow destination $DESTINATION $PORT
sflow polling-interval 10
sflow sample $SAMPLING-RATE
!
```

By default the global enabled sflow will export the flow from all interfaces.

To disable the flow export on specific interface the #no sflow enable# is used in interface config mode #(config-if)

### Mikrotik:

```
ip traffic-flow set interfaces=$ISP cache-entries=1M enabled=yes active-flow-
timeout=5 inactive-flow-timeout=60
ip traffic-flow target set dst-address=$NFA_IP port=2055 src-address=$ROUTER_IP
version=9 v9-template-refresh=100 v9-template-timeout=300
```

### Huawei NetStream:

#### 1. Configure NetStream sampling

```
[Router] interface <$upstream_interface>
[Router-$upstream_interface] ip netstream sampler fix-packets 1200 inbound
[Router-$upstream_interface] ip netstream sampler fix-packets 1200 outbound
[Router-$upstream_interface] quit
```

#### 2. Configure NetStream flow aging

```
[Router] ip netstream timeout active 20
[Router] ip netstream timeout inactive 100
[Router] ip netstream tcp-flag enable
```

3. Configure NetStream original flow statistics exporting

```
[Router] ip netstream export source $router_source_IP  
[Router] ip netstream export host $NFA_IP 2055
```

4. Configure the version for the exported packets

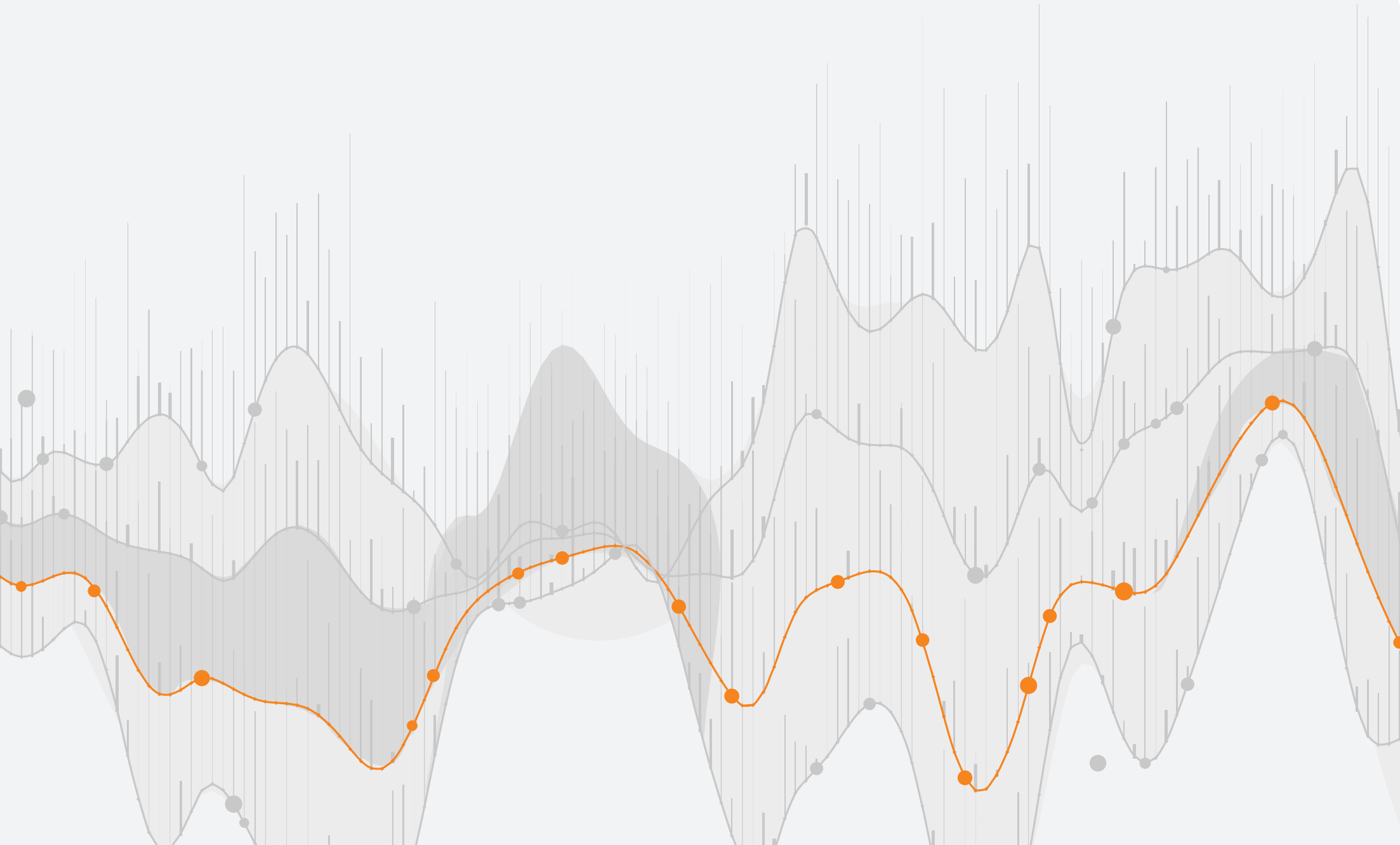
```
[Router] ip netstream export version 9
```

5. Enable flow statistics collection on the interface

```
[Router] interface <$upstream_interface>  
[Router-$upstream_interface] ip netstream inbound  
[Router-$upstream_interface] ip netstream outbound  
[Router-$upstream_interface] quit
```



**NOCTION**  
NETWORK INTELLIGENCE



# Noction Flow Analyzer

## DOCUMENTATION

Copyright ©2025 Noction Inc., All Rights Reserved. Noction logos, and trademarks or registered trademarks of Noction Inc. or its subsidiaries in the United States and other countries.

Other names and brands may be claimed as the property of others. Information regarding third party products is provided solely for educational purposes.

Noction Inc. is not responsible for the performance or support of third party products and does not make any representations or warranties whatsoever regarding quality, reliability, functionality, or compatibility of these devices or products.

**Copyright ©2025 Noction Inc.**