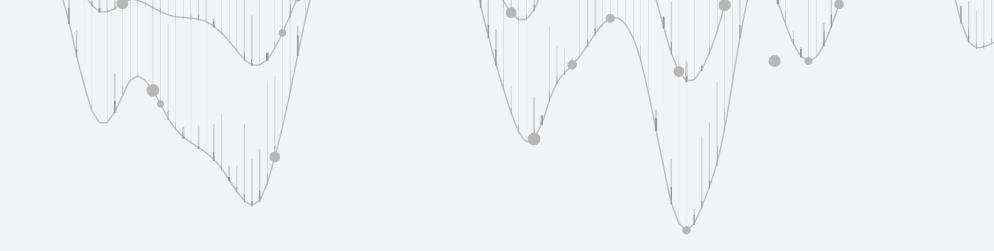




Noction Flow Analyzer DOCUMENTATION



Copyright ©2024 Noction Inc.



Table of Contents

1. NFA Overview	
1.1 NFA Components	
1.2 Collector.	
1.3 Databases	
2. NFA Functionality	
2.1 Frontend	
2.1.1 Dashboards	
2.1.2 Widgets	10
2.2 Data Explorer	
2.2.1 Group & Order	
2.2.2 Filters	
2.2.3 Filtering by Devices	
2.2.4 Time Intervals	
2.2.5 Percentile reporting	
2.3 BGP Data	
2.3.1 BGP Report	
2.3.2 BGP Sankey Diagram	
2.4 SNMP Data	
2.5 Alerts	
2.5.1 Creating Alerts	
2.5.2 My Alerts	
2.5.3 Active Alerts	
2.5.4 History of Alerts	
3. Management	
3.1 Inventory	
3.1.1 Adding Devices	
3.1.2 Managing Devices	
3.1.3 Deleting Devices	
3.2 Configuration Settings	29
3.3 Custom Groups	
3.4 Dictionaries	
3.4.1 MAC Addresses	
3.4.2 PTR Records	
3.5 System Notifications	
3.5.1 System Notifications Overview	
3.5.2 System Notification Channels Configuration	
3.5.3 System Notification Subscriptions	
3.5.4 Notification Text Details	
3.6 User Management and User Directories	
3.5.1 User Management	
3.5.2 LDAP User Directories	
3.7 SSL/TLS Certificates	
3.8 Personalization	
3.9 License Status	
3.10 API Documentation	
3.11 NFA Version	
3.12 NFA Changlog	
3.13 Billing Info	
4. User Profile	
5. System Requirements	41
6. Support	
7. Flow export configuration on network devices	۲۱. ۸1

NFA Documentation

Page 2 of 47

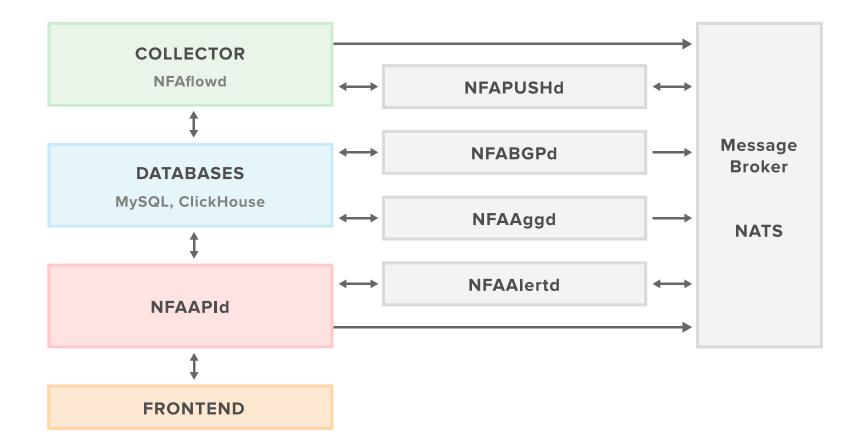


1. NFA Overview

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

NFA Documentation

Page 3 of 47



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.

NFA Documentation

Page 4 of 47



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.

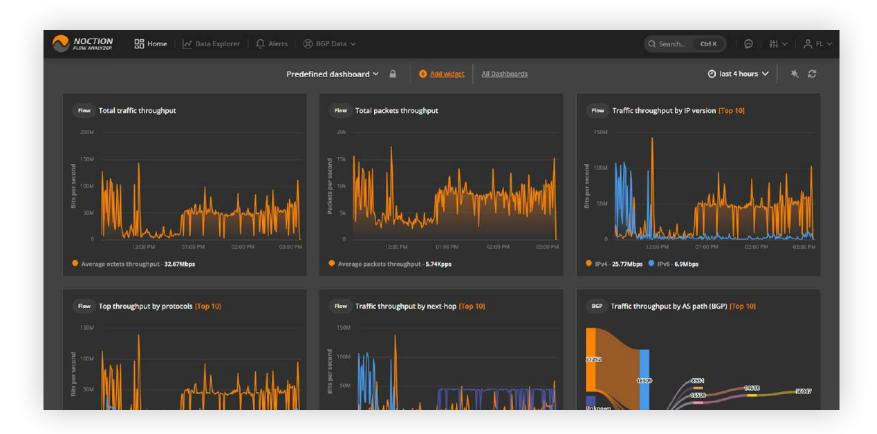
NFA Documentation

Page 5 of 47

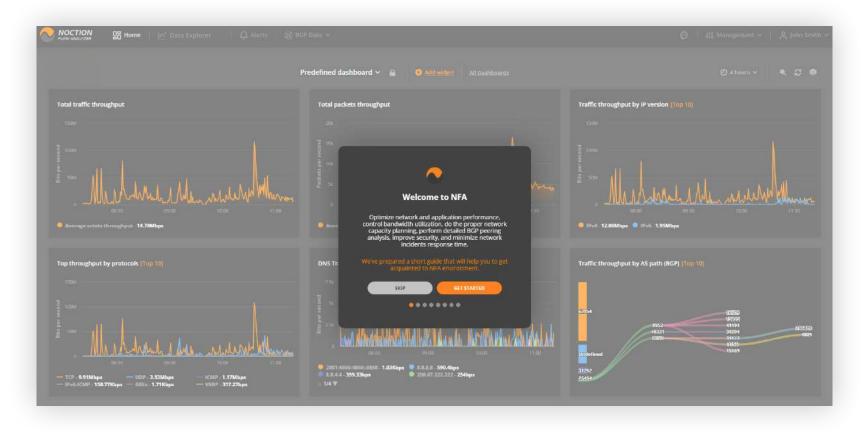
2. NFA Functionality

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.

NFA Documentation

Page 6 of 47



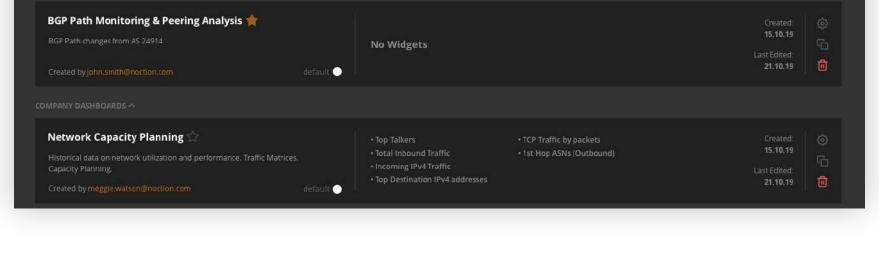
2.1.1 Dashboards

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.

NOCTION 🔠 Home 📈 Data Explorer 🗸	🗘 Alerts [25] 🕃 BGP Data ~		⊖ 뷰 Management∨ 옷 J	
Dashboards > All Dashboards () CREATE NEW DASH	IBOARD		Q Search Dashboards	
Performance Overview 🏠	Bandwidth by Providers Total Inbound Traffic Too Conversations	ICMP Traffic by packets Ist Hop ASNs (Outbound)	Created: 15.10.19 Last Edited:	@ 6
	Top Conversations			



NFA Documentation

Page 7 of 47



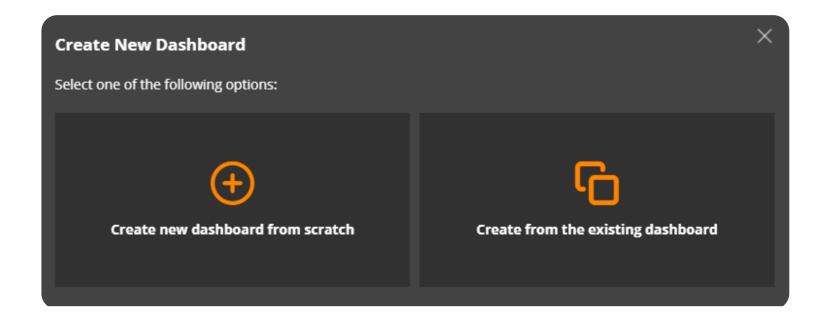
Dashboards are grouped for easy access into recent, favorite and all. For each dashboard, the directory displays the following information:

- 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

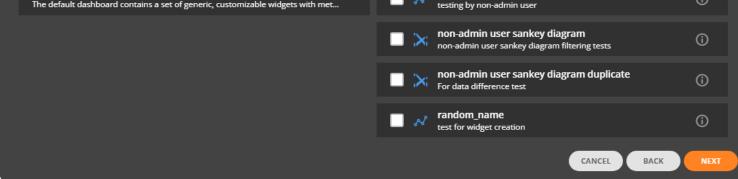
You can easily create a new dashboard in NFA from the All Dashboards directory.

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.

Create New Dashboard					×
Select an existing dashboard to build a new one from:					
non-admin user's dashboard For non-admin user capabilities tests	>		Destination Country Test for Destination Country (is not Moldova) filter, created by	í	
Predefined dashboard		1	IPv6 testing filter by user	ŵ	

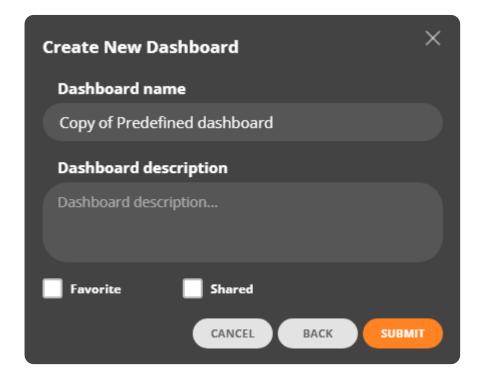


NFA Documentation

Page 8 of 47



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.



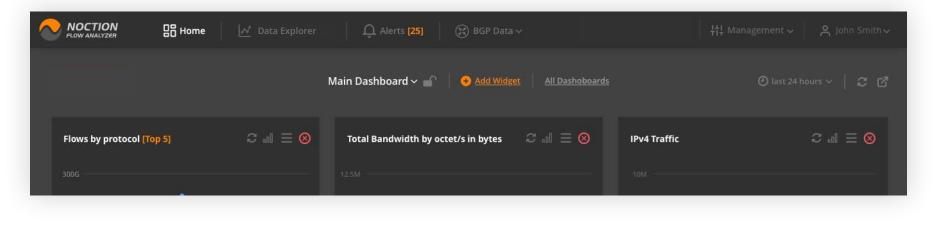
Alternatively, you can create a new dashboard by cloning an existing one in the All Dashboards directory.

NOCTION BHOME Data E	xplorer 🛛 🗍 Alerts [25] 🛛 🛞 BGI	P Data	井 Management ~ 은 John	Smith∽
Dashboards > All Dashboards 💮 CREATE NEWS	ASHBOARD		Q Search Dashboards	
PERSONAL DASHBOARDS A	Bandwidth by Provide Total Inbound Traffic Total Conversions	ers • ICMP Traffic by packets • 1st Hop ASNs (Outbound)	15.10.19	0 6
Created by john.smith@noction.com	• Top Conversations • Flows by Protocol default		Last Edited:	۵

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.



NFA Documentation

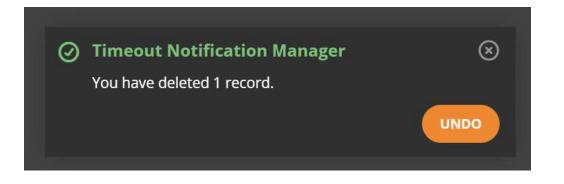
Page 9 of 47



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.

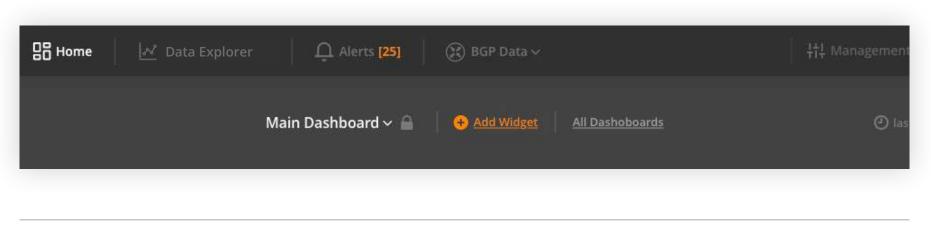


2.1.2 Widgets

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.

	Main Dashboa	ard 🛩 🔒 🛛 😣 Add		
Flows by prot	All Widgets	Company [24] Per	Q s	earch Widgets
ado. Nos	Flows by protocol Summary of flow Protocols Jorem (psum dolor sit amet	0 6	Top Destination ASNs Summary of flow Protocols lorem ipsum dolor sit am	et O G
575	Summary of flow Protocols forem (psum dolor sit amet	• •	Summary of flow Protocols lorem lpsum dolor sit am	" © ©
	Countries Summary of flow Protocols Jorem (psum dolor sit amet	⊙ ि ⊗ □	Bandwidth by Providers Summary of flow Protocels lorem ipsum deler sit am	. 060
.0	BGP Sankey Ultra Really Long Name Summary of flow Protocols foram (psum dolor with	⊙ ₲ ⊗ 🗧	BGP Sankey 2 summary of flow Protocols lorem lpsum dolor sit am	et 🛈 🔂 🔕
— Ter	BGP Sankey Ultra Really Long Name Summary of flow Protocols forem (psum dolor with	06⊗ □	Bandwidth by Providers Summary of New Protocols Iorem (psum dolor sit am	. O G ⊗
	CREATE NEW WIDGET		Summary of now Process for an ipsoin boot sit an	D TO DASHBOARD

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



NFA Documentation

Page 10 of 47

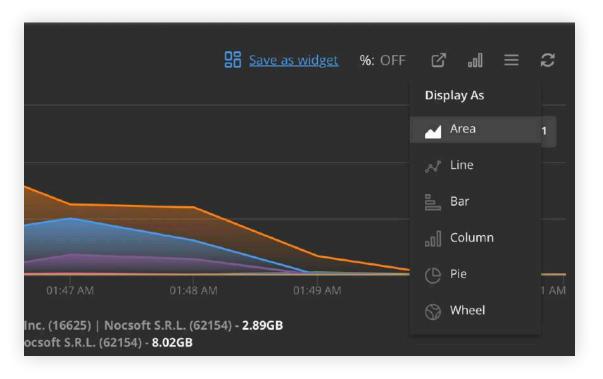


You can easily create a new widget from scratch by proceeding to **Data Explorer** in the top menu, selecting the filtering and grouping options and subsequently saving the Data Explorer view as a new widget to the desired dashboard.

NOCTION BR Home Mata Explorer	. Alerts	◎ 指: Management ~ 名 John Smith ~
🔀 Hide Query Parameters		
III Octets - Advanced Options Save My Filters	Throughput in bytes 🗸	B [®] Save as widget %: OFF D [®] all
Ø last 4 hours ∨ RUN QUERY		
🍸 Filters 🚍 Narrow By 📈 Group & Order	1 500 4	
AND OR 🕂	<u><u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u></u>	
Protocol T	Mhommhluhhannel	montant
TCP (6) ×	одиз РМ Своб РМ Св.15 РМ Св.30 РМ Св.45 РМ С4.45 РМ С4.45 РМ С4.45 РМ С4.45 РМ С4.45 РМ С5.15 Р Ф Тhreughput 39.89G8	NA 05:50 PM 05:43 PM 06:00 PM 06:13 PM 06:30 PM

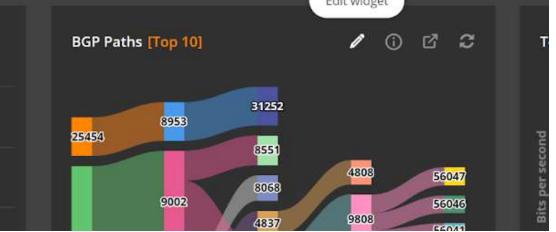
Alternatively, you can create a new widget by duplicating an existing one. Click on the existing widget name to open it in **Data Explorer**. Make desired modifications and save it as a new widget.

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.

Edit widget



NFA Documentation

Page 11 of 47



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.

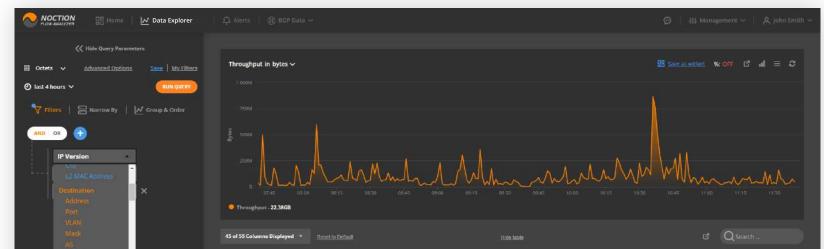
Data Explorer takes the ensuing statistics from the DB table Flows which includes but is not limited by the following:

- Time
- Source and Destination Address
- Source and Destination Port
- Source and Destination VLAN
- Source and Destination Mask
- Source and Destination AS Number L3 IP TTL
- 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 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.



Country, City	IP Version	Source Address	Destinution Address	Protocol	Input Interface	Output Interface	Src. Mask	Sec. AS	Total	Total	Total	Src. Country	Dest. Country	Sec. City	Dest. City
	ipvdi	99.102.219.0	185.34.202.193	юмр	561	570		7018	6.8KB	100 packets	1 flows	US	NL	Reno	Hall
	ipv4	95.65.8.138	185.34.202.89	юмр	561	569	18	31252	22.4KB	400 packets	1 flows	MÐ	NL.	Chisinau	Hall
	ipv4.	95.65.8.138	185.34.202.83	ICMP	561	569	18	31252	5.6KB	100 packets	1 flows	MD	NL	Chisinau	Hall
	ipvd	95.65.8.138	185.34.202.186	ICMP	561	570	18	31252	33.6KB	600 packets	1 flows	MD	NL	Chisinau	Hall
	ipv4	95.65.8.138	185.34.202.145	ICMP	561	570	18	31252	28KB	500 packets	1 flows	MD	NL	Chisinau	Hall

NFA Documentation

Page 12 of 47



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 select the Ingress, Egress, or a combined view of the AS traffic.

To hide/show specific table columns, click the corresponding "Hide/Show Columns" dropdown option and checkmark the items of interest.

	1 Alerts 🔰 🕄 BGP Data 🗸	ଡ଼ା #~ ዳ୍ୟ~
Hide Query Parameters Octets Advanced Options Save My Filters Jast 4 hours	Throughput [Top 10]	명중 Save as widget %: OFF 더 all 프 37
😽 Filters 🛛 🖯 Narrow By 🗍 🗽 Group & Order	acon -	
IP Version	Advanced Options Show Top: 10	
IPv6 * ×	3 - 6.321 Limit Table to: 300 3 of 69 Colum AS Traffic Direction: GENERAL INGRESS EGRES	-6.71MB • 540 -61.07MB • 0 - 1.34MB • 41 - 13.94KB
		PLY Minimum Maximum 245.25KB 441.31MB
		3.9G8 305.19KB 208.72MB

NFA Documentation

Page 13 of 47



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.

NOCTION BE Home M Data Explorer	l Alerts 🛞 BGP Data 🗸					☺ # ▾ 옷℡▾
K Hide Query Parameters					05	an a 1 - a
III Octets V Advanced Options Save My Filters	Throughput [Top 10]				BE Save as widget %	off ⊠ al ≡ ⊅
O last 4 hours Y RUN QUERY						
🏹 Filters 🛛 🖶 Narrow By 🕴 🛃 Group & Order	1 500M			'nh		
UNIDIRECTIONAL BIDIRECTIONAL	500M				- 1 A	
Select Grouping Criteria	0 2515 FM 02150 FM	02:45 PM 02:00 PM	CATERN OS:40 PM 03:45 PM OR:00		04/45 PM 05/00 PM 05/15 PM	
Grouping Order:	Fastiy, Inc. (54113) - 3.17GB StarNet Solutii SRL (31252) - 2		ogle LLC (15169) - 10.28GB ple Inc. (6185) - 673.73MB	Cloudfiare, Inc. (13 Amazon.com, Inc. (
Source AS ×	1/3 V	1.1900	pre (nc. (0103) - 0/3./3MB	Amazon.com, inc. (10:10: - 0.0200	
Order by octets	5 of 67 Columns Displayed 🛛 🔻		Hide ta			Q Search
Percentaine Procession	Line color	Src. AS	Source As Name	Total	Minimum	Maximum
Prefix Grouping:	<u> </u>	31252	StarNet Solutii SRL	27.19GB	10.97MB	729.21MB
Group by Source Prefix Group by Destination Prefix	•	15169	Google LLC	10.28GB	859.15KB	1.14GB
	۰.	13335	Cloudflare Inc.	6.77GB	12.03KB	1.07GB

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.

Prefix Gro	uping:	Line co
🧧 Group by Source Prefix 🛛 🚦	Group by Destination Prefix	
Source /17	×	
Destination /17	×	
		•

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.

NFA Documentation

Page 14 of 47



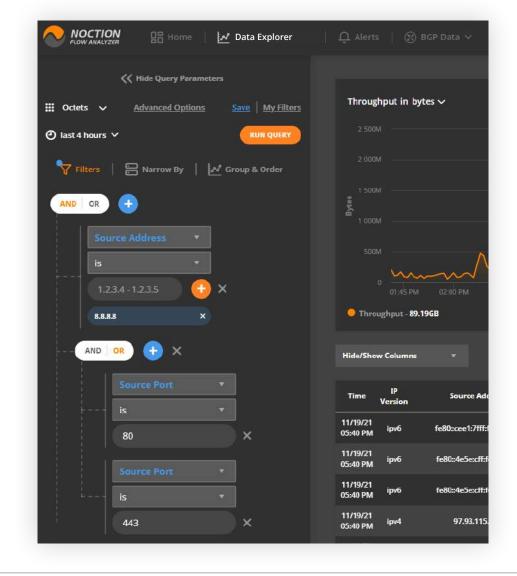
NOCTION III Home M Data Explorer						
It Octets Advanced Options Save My Filters Isat 4 hours Isat 4 hours Isat 4 hours Isat 4 hours Isat 4 hours Isat 4 hours Isat 6 hours Isat 7 hours Isat 4 hours Isat 7 hours Isat 7 hours Isat 7 hours Isat 4 hours Isat 7 hours Isat 7 hours Isat 7 hours Isat 4 hours Isat 7 hours Isat 7 hours Isat 7 hours Isat 7 hours Isat 7 hours Isat 7 hours Isat 7 hours Isat 8 hours Isat 7 hours Isat 7 hours Isat 7 hours	test order 2 [Top.10]			 StarNet Solutili SRL (\$1252) Arnazon.com, inc. (15394) Google LLC (\$1509) Google LLC (\$1509) Horst Limeter (\$1540) Horst Limeter (\$1540) Horst Limeter (\$1550) Horst Limeter (\$1515) Horst Limeter (\$1515) Clauditation I, Clauditation I, Akamal Technologies, Inc. 	Nocsoft S.R.L. (62154) Nocsoft S.R.L. (62154) ff S.R.L. (62154) iont S.R.L. (62154) - 1 iont S.R.L. (62154) - 1 S.R.L. (62154) - 1 26222) Nocsoft S.R.L foc. (3356) / Nocsoft S.R. ocsoft S.R.L. (62154) -	- 12.17G8 5.32G8 -6.22G8 G8 9GB 12154) - 2.95G8 L. (62154) - 2.73G8 2.3G8
Order by Octets v	8 of 67 Columns Displayed				er Qr	
Descending Order *	Line color	A5 (A)	AS (B) Total	Total from (A) to (B) Total from (B) to (A)	Minimum	Maximum
		31252	62154 23.94GB	22.77GB 1.17GB	339.86KB	1.11GB
		16509	62154 12.17GB	12.17GB 7.11MB	387.73KB	2.43GB
		15169	62154 6.32GB	5.87GB 447.65MB	656.49KB	301.87MB
		25462	62154 6.22GB	6.22G8 08	520B	991.95MB

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.



NFA Documentation

Page 15 of 47

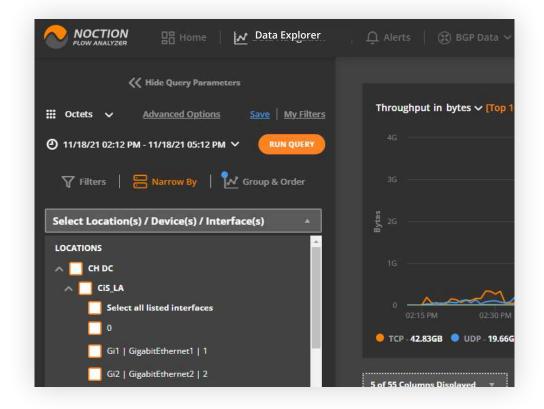


2.2.3 Filter by Locations, Devices and Interfaces

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.



<		Octo	ober	2021					Nove	mbei	r 2021		
				1	2	3	1	2	3	4	5	6	7
4	5	6	7	8	9	10	8	9	10	11	12	13	14
11	12	13	14	15	16	17	15	16	17	18	19	20	21
18	19	20	21	22	23	24	22	23	24	25	26	27	28
25	26	27	28	29	30	31	29	30					

NFA Documentation

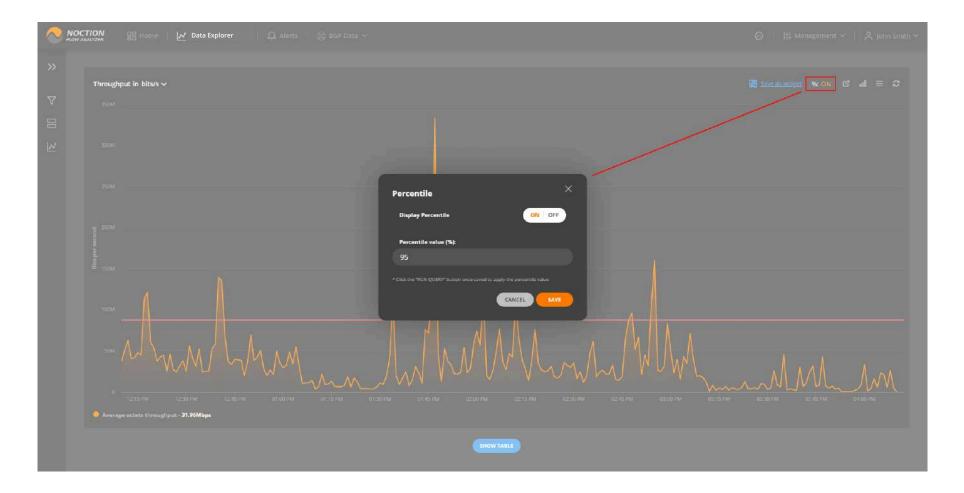
Page 16 of 47



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.

NFA Documentation

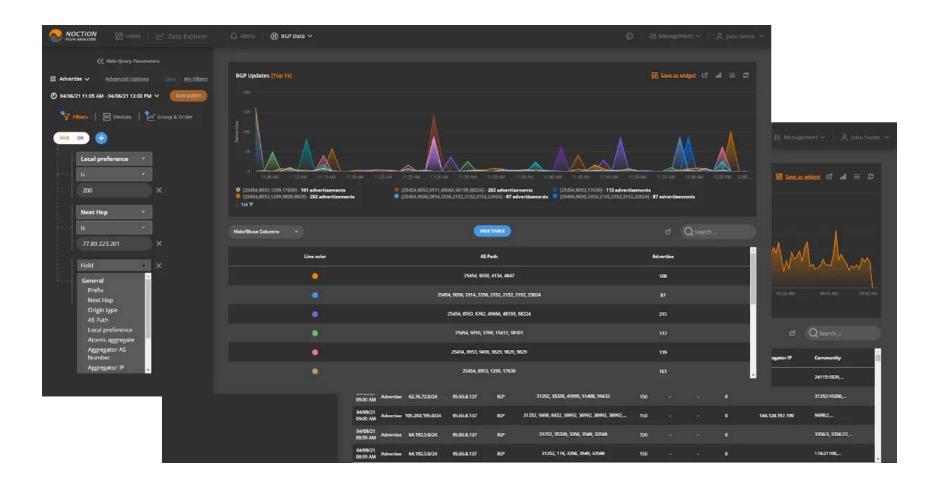
Page 17 of 47



2.3.1 BGP Report

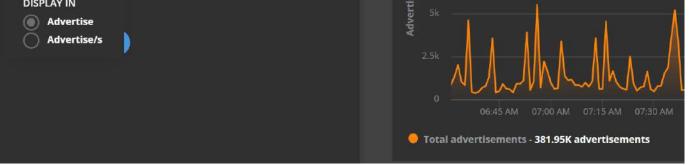
Use the BGP Report section to see BGP data obtained from your devices. The BGP Route advertisements and withdrawals can now be visualized both in a graph and table mode.

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.

NOCTION III Home At Explorer	🕂 Alerts 🛛 🕃 BGP Data 🗸
K Hide Query Parameters	
III Advertise V Advanced Options Save My Filters	BGP Updates
AGGREGATE BY Advertise RUN QUERY	
◯ Withdraw ◯ Route	
	e e e e e e e e e e e e e e e e e e e



NFA Documentation

Page 18 of 47



2.3.2 BGP Sankey Diagram

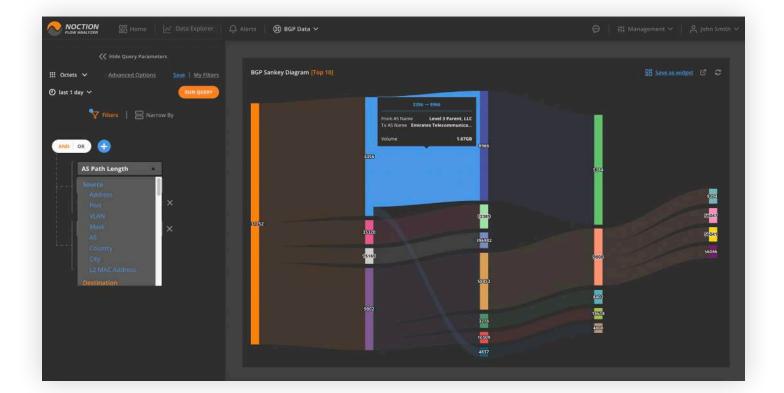
NFA offers a great way to visualize the Internet traffic routing criteria along with traffic volume using a Sankey type diagram. Its extensive filtering capabilities can provide you with a clear picture of the paths your traffic is taking, the countries regions or cities you traffic originates and terminates 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** ٠
- Source and Destination Port
- Source and Destination VLAN
- Source and Destination Mask
- Source and Destination AS Number L3 IP TTL
- 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

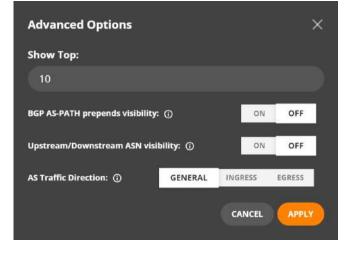
- MPLS VPN Route Distinguisher
- MPLS Top Label TTL
- MPLS Label Stack Length
- MPLS Label Stack Depth
- MPLS Top Label Exp
- L3 IP min TTL
- L3 IP max TTL
- L3 IP Total Length
- L3 IP min Total Length
- L3 IP max Total Length
- **BGP Community**
- TOS Type of Service
- Protocol
- Input Interface
- **Output 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 prepends as well as the upstream/downstream ASNs info, and select the Ingress, Egress, or a combined view of the AS traffic.



NFA Documentation

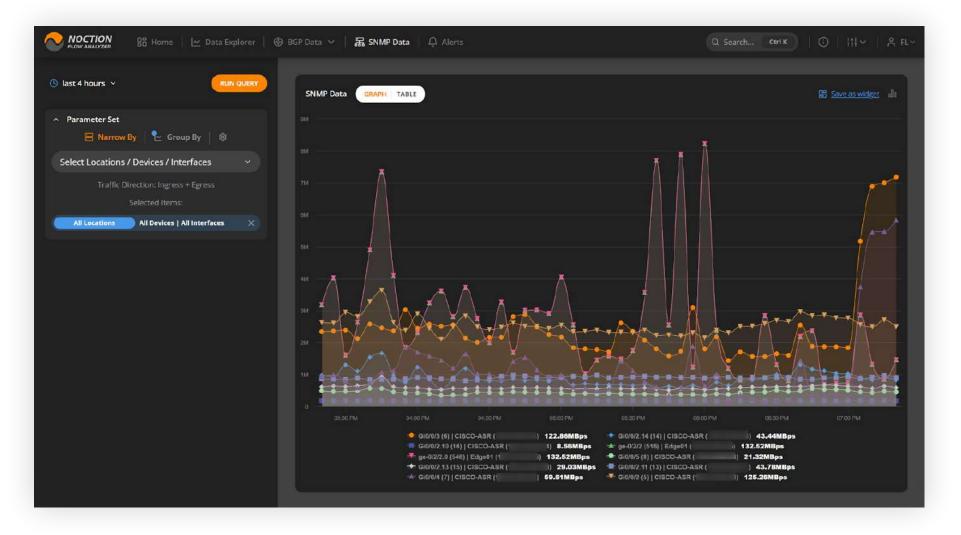
Page 19 of 47



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.



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

ROUTION BB Home 🗠 Data Explorer 🤅	🛿 BGP Data 〜 品 SNMP Data ့ Alerts			Q Search	Ctri K	iliv A FL∘
() last 4 hours ~ RUN QUERY	SNMP Data GRAPH TABLE					
∧ Parameter Set □ Nammer By Use Group By 0	Interface SNMP Index Agent Address	Minimum	Maximum	Average	Total	95th Percentile
	🗸 Gl0/0/3 (6) CISCO-ASR ()	674.18KBps	18.28MBps	6.76MBps	331.22MBps	17.3MBps
Select Grouping Criteria	✓ Gi0/0/2.14 (14) CISCO-ASR ()	629.61KBps	1.05MBps	771.54KBps	37.81MBps	994.66KBps
Grouping Order:	✓ Gi0/0/2.10 (16) CISCO-ASR ()	165.68KBps	228.34KBps	177.33KBps	8.69MBps	185.49KBps
General Interface SNMP Index ×	✓ ge-0/2/2 (516) Edge01 ())	430.41KBps	6.2MBps	1.53MBps	75.04MBps	3.89MBps
General Agent Address X	✓ ge-0/2/2.0 (546) Edge01 ()	430.36KBps	6.2MBps	1.53MBps	75.04MBps	3.89MBps
	🤝 Gi0/0/5 (8) CISCO-ASR ()	345.64KBps	474.89KBps	388.04KBps	19.01MBps	436.81KBps
Parameter Set Narrow By Croup By Select Grouping Criteria Grouping Order: Grouping Order:	🤍 Gi0/0/2.13 (15) CISCO-ASR ()	479.5KBps	564.04KBps	513.98KBps	25.19MBps	546KBps
	🤟 Gi0/0/2.11 (13) CISCO-ASR ()	222.77KBps	412.73KBps	281.72KBps	13.8MBps	346.9KBps
	✓ Gi0/0/4 (7) CISCO-ASR ()	55.5KBps	17.74MBps	6.2MBps	303.91MBps	16.57MBps
	✓ Gi0/0/2 (5) CISCO-ASR ()	1.53MBps	2.07MBps	1.75MBps	85.79MBps	2.01MBps

NFA Documentation

Page 20 of 47



Click the **Gear icon** to open up Settings. 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.

NOCTION 🔠 Home 🗠 Data Explorer	⑧ BGP Data >
(S) last 4 hours ~ RUN QUERY	SNMP Data GRAPH TABLE
 ^ Parameter Set 금 Narrow By ∠ Group By Ø Metric: ① 	40M
octets/s	35M
auto	30M
10	20M
	15M

NFA Documentation

Page 21 of 47



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**.

NOCTION 🗄 Home 🛛 🗠 Data Explorer 🛛 🗘 Alerts 🖉 BGP Data 🗸		₽ ₩ ~ Զ п. ~
	New Alert	
ALERT NAME:	Configuration O Alert Details = Alert Summary ALERT DESCRIPTION:	
Bandwidth Usage Close to Commit ALERT PRIORITY:		
High Priority		

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

ALERT TRIGGER CONDITIONS		
ADD RULE		G Duplicate
SELECT DEVICES Select Devices *	Paris DEV2 ×	
SELECT GROUP CRITERIA ① Source City	Destination Prefix	
FILTERS CRITERIA ① AND OR +		
Source Country * is	France	×
Destination Port • is	* 881	• ×



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

USE COMPLEX LOGIC	

NFA Documentation

Page 22 of 47



4. 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**.

CONDITION(S) MUST EXIST FOR MORE THAN					ie.			
0	0	Seconds		8	IN		8	Seconds 🔻
						500000000000000000000000000000000000000		

5. 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.

	New Alert
Alert Threshold Configuration	📮 Alert Details 🚍 Alert Summary
ACTIVATION OPTIONS:	SNOOZE ALERT NOTIFICATIONS
Activate on date/time • 04/11/22 12:24 PM	Day of the week: Snooze alert for:
INTERVAL BETWEEN NOTIFICATIONS:	Sunday 🔹 All day 🔹 🕞 ADD SNOOZE
0 😝 Minutes 🔻	DESTINATION: (Email / Slack)
RESET ALERT:	Destination
Reset on next check if no longer true (Recommended) *	Jane.doe@noction.com
	support@noction.com
	SHARED ALERT:
	(All users can view. Admin can edit/delete this alert).

6. 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.

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

NFA Documentation

Page 23 of 47



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.

	ifications	Active Alerts	Ay Alerts 📃 🚝 History of Alerts			
Q Search	Alerts			Sort by	Priority 🗸 💽	CREATE NEW ALERT
On/Off	Name		Last Edited	Created	Created by	Actions
	Bandwidth Level Close to Commit		10.25.15	10.22.19	Alex Williams	0 6 8
	Bandwidth Level Close to Commit lorem ips	um delor cit amer	10.24.19	10.17.19	John Smith	168

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.

lerts & Notifications	Active Alerts	History of Alerts			
Q Search Alerts	19 Critical 129 High	209 Low			Sort by <u>Priority</u>
Alert Name		Triggered at	Created by		Actions
Bandwidth Level Close to Commit in London Data Center		10:07 AM 10.22.19	Alex Williams	<u>View Details</u> ∨	/ RESET
Potential BGP Hijacking of AS12345		12:18 PM 10.21.19	John Smith	View Details 🗸	RESET

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.

lerts & Notifications	Active Alerts 🕺 My A	Alerts History of Alerts			
Q Search Alerts				Sort by Pri	ority
Alert Name		Triggered at	Owner	Act	tions
Bandwidth Level Close to Commit		10:07 AM 10:22.19	Alex Williams	View Details	8
High Level of TCP traffic forem ipsum dolor sit amet		12:07 AM 10.22.19	John Smith	View Details	8
Traffic Lorem Ipsum dolor amet		11:07 AM 10.22.19	Alex Williams	View Details	8

NFA Documentation

Page 24 of 47



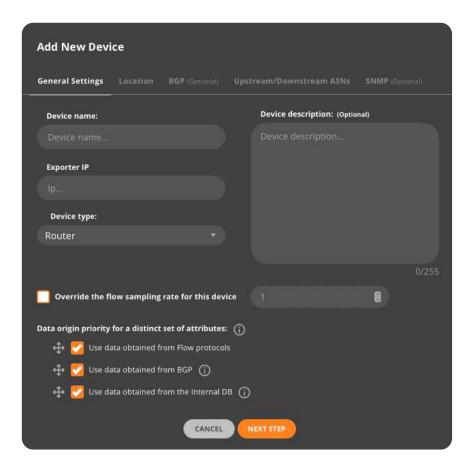
3. Management

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.

Management Panel > Inventory San Francisco (4 Devices)	Devices	Locations	Inventory Configuration Settings System Notifications User Management
✓ R25-SF Flow: ⊘ BGP: ⊘	Q ON OFF	✓ R25-LD Flow: ⊘	License Version Billing Info
∨ R17-SF Flow: (!) BGP: ⊘	ON OFF	✓ R26-LD Flow: () BGP: ()	
∨ R17-SF Flow: ① BGP: ⊗	C / ON OFF	✓ R27-LD Flow: ① BGP: ⊘	Q / ON O
∨ R17-SF Flow: (!)	ON OFF		

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.

NFA Documentation

Page 25 of 47



Add New Device		
General Settings Location		Upstream/Downstream ASNs SNMP (Optional)
Choose existing location:		
none		OF CREATE NEW LOCATION
Location name:		Description: (Optional)
		Description
Country: (Optional)		
City: (Optional)		0/255 State/Region: (Optional)
		State/Region
Phone number: (Optional)		Address: (Optional)
		Address
Upstream ASNs		Downstream ASNs
0 - 4294967295		0-4294967295
	CANCEL	IACK NEXT STEP

		BGP (Optional)		
		Use BGP da	ita from this device	
			' data from another is already set to IFA	
		🔘 No BGP dat	a from this device	
Our AS: (Optional)	D		Our address: (Optional)	
Our AS			Our address	
Peer AS:			Peer address:	
Router ID: (Optional			Password: (Optional)	
Router ID				
BGP Session		ON OFF		

Add New Devi	ice			
General Settings		BGP (Optional)	Upstream/Downstream ASNs	SNMP (Optional
		🔘 Use BGP d	ata from this device	
			P data from another t is already set to	

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

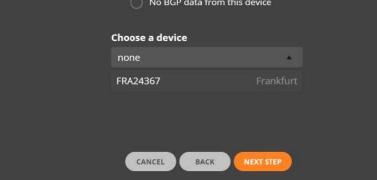
Enabling BGP data export from the device you are about to add is optional.

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.

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"

NFA Documentation

Page 26 of 47



Add New Device			
General Settings Locatio	n BGP (Optional)	Upstream/Downstream ASNs	SNMP (Optional)
Use the location's Ups Use specific Upstream			
Upstream ASNs		Downstream ASNs	
0 - 4294967295	(ADD	0 - 4294967295	
12 / X		21 🖉 🗶	
	CANCEL	BACK NEXT STEP	

Add New Device

General Settings
Location

No SNMP
BGP (Optional)

No SNMP
SNMP v2c

No SNMP
SNMP Username

SNMP Host Address
SNMP Username

SNMP Host Address
SNMP Context name (Optional)

Security Level
SNMP Context name (Optional)

noAuthNoPriv
SNMP Context name

SNMP Encryption
Authentication Protocol

SNMP Encryption
Authentication Password

BACK

CANCEL

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.

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.

NFA Documentation

Page 27 of 47



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.

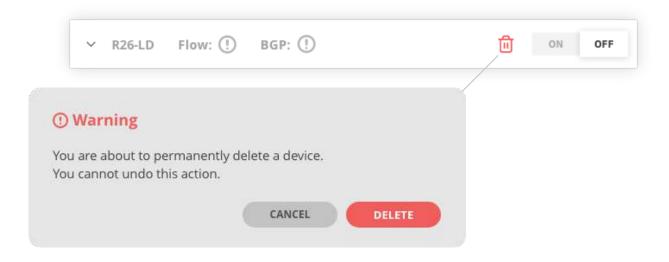
∧ DEV1	Flow: 🥑 🛛 BC	iP: ⊘ S	SNMP: 🥝	~ `× /	ON OFF
ON	OFF BGP 185.34	.202.246 -	Established conn	ection	
ON	OFF SNMP (1		The last request v	vas finished wi	th success
Status	Exp. IP	Exp. ID	Sampling Rate	Flow Type	Flow Rate
•	185.34.202.233	0	1	netflow	20 flows/s
	185.34.202.233	589824	10	ipfix	4 flows/s
•	185.34.202.233	524288	10	ipfix	10 flows/s
۲	185.34.202.233	256	1	netflow	273 flows/s
•	185.34.202.233	666666	1	ipfix	1 flows/s

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.



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.



NFA Documentation

Page 28 of 47



3.2 Configuration Settings

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

anagement > Configuratio	o sertines						
API				LOGS			
SSL	Disabled Enabled	SSL redirect	Disabled Enabled	APId log level		BGPd log level	
SSL listening IPv4/IPv6 add	ress	SSL listening port		info	*)	(info	
#× Add ip		443	:)	Aggd log ievel		Flowd Log level	
Non-SSL IPv4/IPv6 listening	addrare .	~		(info	•)	(info	6
** Add ip	autress	Listen port	.)	Alertd log level		Pushd log level	
(and hour p				info	•)	(info	
		Allowed IP addresses					
Front-end access restriction	Disabled Enabled	0.0.0.0 × 0.0.0 × A	dd cidr				
Worker threads				STATS			
5 0	(٢			Collector data1 granularity	(minutes)	Collector data1 keep time (n	ninutes)
				(1	•)	(1440	
FLOW COLLECTOR				Collector data2 granularity	(minutes)	Collector data2 keep time (n	ninutes)
				5	0)	11520	1
NetFlow/J-Flow/NetStrea	m/IPFIX listening port	sFlow listening port		Collector data3 granularity	(minutes)	Collector data3 keep time (n	ninutes)
2055	۵)	6343	۵)	(10	:	576000	

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

NFA Documentation

Page 29 of 47



- 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 SNMPId. 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

NFA Documentation

Page 30 of 47



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

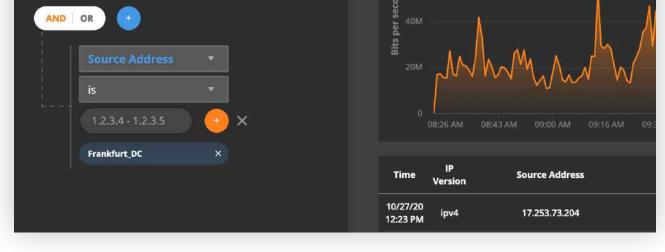
3.3 Custom Groups

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.

PLOW AN	TION 답답 Home [관 Data Explor							
Manage	ment > Custom Groups							
						Custom Groups		
Q Sear							CUSTOM GR	OUP
1	Name 🛦	Description	Туре	Last Edited	Cr		Actions	
<u> </u>			1364	Last Lonco			Actions	
	Frankfurt_DC	Frankfurt DC	ip	10/26/20 12:54 PM	Joł			
	London	UK London plant IPs	ip	10/26/20 12:41 PM	Joł	n Smith		
3	Tokyo_DC	Tokyo Data Center	ip	10/26/20 05:24 PM	Jot	n Smith	/ 6 6	

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

NOCTION FLOW ANALYZER Home At Data Explorer	💭 Alerts 🛞 BGP Data 🗸
Hide Query Parameters	
III Octets V Advanced Options Save My Filters	Throughput in bits/s \checkmark
④ 10/27/20 08:26 AM - 10/27/20 12:26 PM ∨ RUN QUERY	80M
🍸 Filters 🚍 Devices 📈 Group & Order	60M



NFA Documentation

Page 31 of 47



3.4 DICTIONARIES

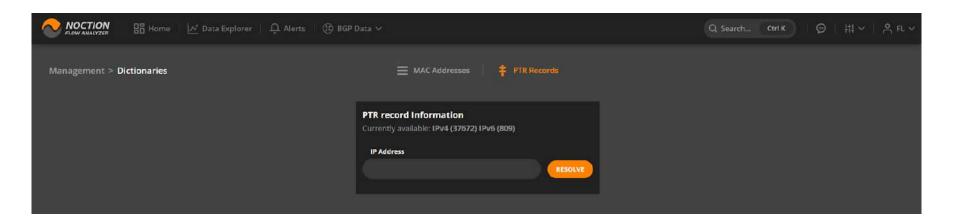
3.4.1 MAC Addresses

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.

	ome 🛛 🖉 Data Explorer	유 Alerts 🛛 🔅 BGP Data 🗸			Q. Search	Ctrl K) # ~	FL ∨
Management > Dictiona	ries		E MAC Addresses	📫 PTR Records				
Q Search MAC address								
2b:3c:4d:5e:6f:7a								

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

NFA Documentation

Page 32 of 47



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.**

	a Explorer 📮 Alerts 🛞 BGP Data	~		Q Search Ctrl K ⊖ H ✓ A FL ✓
Management > System Notifications		Notification Subscriptions	Notification Channels	
🔀 Email Channel Configuration				Shared Email Configuration
From: Port: root@localhost 25	Host: localhost	Encryption: none	CHANGE	RESET
╡ 봄 Slack Channel Configuration				Shared Slack Configuration
Slack bot name:	Slack avatar emoji:	Slack avatar url:	Slack URL:	RESET
NFA	:robot-face:			UPDATE
C Mattermost Channel Configuratio	n			Shared Mattermost Configuration
Mattermost username:	Mattermost avatar emoji:	Mattermost avatar url:	Mattermost URL:	RESET
NFA	:robot-face:			
Telegram Channel Configuration	ı			Telegram Channel Configuration
Telegram Bot Token:				RESET
changeme00				UPDATE

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 Slack and Mattermost channels configuration, specify the bot name and URL. For

Telegram, provide the proper bot token.

NFA Documentation

Page 33 of 47



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.

anagement > System Notifications	I Notification Subscr	iptions 🛱 Notification Channels			
Q Search Subscriptions			Sort	oy <u>Created Date</u> ~	CREATE NEW
Subscription Name		Last Edited	Created	Owner	Actions
Core Component Status Subscription		10.25.19	10.22.19	Alex Williams	© / Ø
Weekly TCP Related Alerts Report		10.24.19	10.22.19	John Smith	0/8

Configuration				
TOPIC				
Topic				
DESCRIPTION				
Description				
NOTICE ON COLLOWING FURNIS				
NOTIFY ON FOLLOWING EVENTS		Others		
NOTIFY ON FOLLOWING EVENTS		Other		
	at fermentum magn			•
ma				•
Ma Adipisicing architecto placed				8
Ma Adipisicing architecto placed				•
Ma Adipisicing architecto placed				8
Ma Adipisicing architecto placed			SAV	B
Ma Adipisicing architecto placed		am	SAV	B
Ma Adipisicing architecto placed		am	SAV	B

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,

NTERVAL BETWEEN NOTI		utes): 0	\$
Destination:			
Destination	(⊕ AD	•	
SNOOZE ALERT NOTIFICAT	IONS		
SNOOZE ALERT NOTIFICAT Day of the week:	IONS Snooze alert fo	or:	
		or: T	+ ADD SNOOZ
Day of the week:	Snooze alert fo	ər: •	⊕ ADD SNOOZ
Day of the week:	Snooze alert fo	ər: •	• ADD SNOOZ
Day of the week:	Snooze alert fo	ər: •	⊕ ADD SNOOZ

specify when to Snooze Notifications if desired and hit "Save".

NFA Documentation

Page 34 of 47



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

	CTION 🔡 Home 🛛 🕅 Data Expl	lorer 📮 Alerts 🛞 BGP Data 🗸			9	#∽ _ ≜ □s ∨
	ement > User Management archuser					ADD USER
#	Full Name 🛪	User Name	Email	User Directory	Role	Actions
1	John Snow	jsnow	jsnow@noction.com	internal	admin	/ 8
2	David Smith	admin	admin@noction.com	internal	admin	

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.

NFA Documentation

Page 35 of 47



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

The general tab covers:

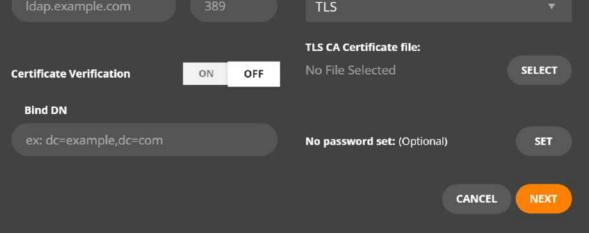
- User directory name the name assigned to the directory within NFA
- User directory type
- State a toggle to enable or disable a user directory,
- Order specifies when this user directory will be examined by NFA compared to other user directories

Add New Directory		>	<
General > Server >			
User Directory Name		User Directories Type	
User Directory Name		LDAP 🔻	
		Order	
State	ON OFF	0	
		CANCEL	

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

Add New Directory		×	
General > Server	> User Schema		
Hostname	Port	Encryption	



NFA Documentation

Page 36 of 47



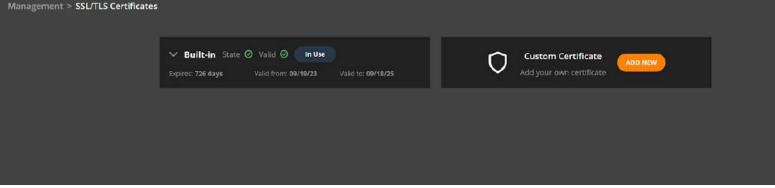
The user schema tab covers:

- 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

Add New Directory	×
General 📏 Server 📏 User Schema	
Directory Type	
Active Directory 🔹	
Base DN	Object Class
	user
Object Filter	Full Name Attribute
(&(objectCategory=Person)(sAMAccount	displayName
Username Attribute	Email Attribute
sAMAccountName	mail
	CANCEL 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**.



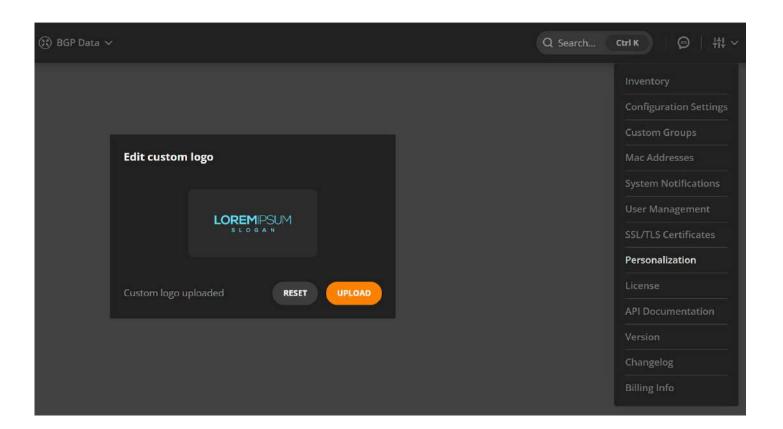
NFA Documentation

Page 37 of 47



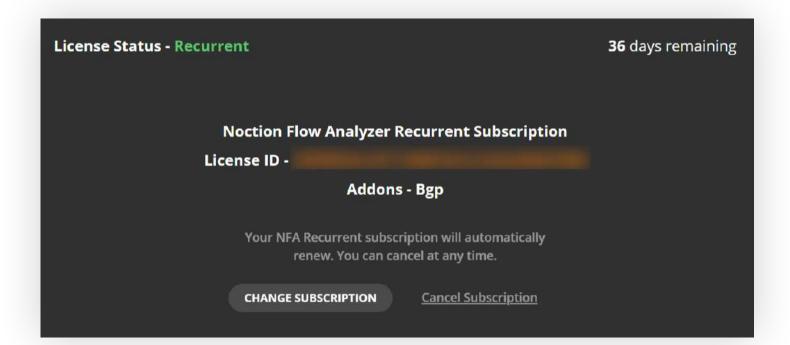
3.8 Personalization

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.

NFA Documentation

Page 38 of 47



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.

NOCTION 🔐 Home 🗠 Data Explorer 🗘 Alerts 🚳 UGP Data 🗸	⊖ ## Management ∨ A jobus Smith ∨
Management > API Documentation	Inventory Configuration Solitings Custom Groups
/alerts (Alerts) /alerts/(id) (Alerts)	System Notifications Uner Management Licente GIT (POST) (DELET)
/alerts/(id)/triggerreset (Mers) /alerts/(id)/enable (Mers)	Api Documentation (Post) Version Billing info
/alerts/triggered (Arrts) /alerts/history (Arrts)	e e
/config:(caregory)(Configuration)	(75) (76) (15)
/config/metadata (Configuration) /customgroups (Custom groups) /customgroups/(id) (Custom groups)	(19) (19) (19) (19) (19) (19) (19) (19)
/dashboards (Tarihomis)	(FO) (FD) (FD) (FD) (FD) (FD) (FD) (FD) (FD
/devices (Instein)	(EC) (TO)

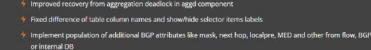
3.11 NFA Version

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.

NOCTION BE Home W Data Explorer Q Alerts 09 BGP Data ~		t‡‡ Management ∽	우, John Smith ~
Management > NFA Changelog 21.11.0 ~ New features and improvements 4 Added ability to view changelog via Frontend 4 Implemented better filtering by device interfaces as well as devices and locations in Data Explorer and Sankey diagram	Bug Fixes Frontend: Fixed validation of email from field in email notification channel Decrease memory footprint of geodata in flowd component Fixed sectors that a channel is a channel in the sector of the sectors of the		
 Added rate unit to Sankey Diagram Display AS Names on Data Explorer Improved order selection of device ASN info origin priority Added ability to enable/disable AS path prepend remove in Sankey diagram 	 Fixed error when changing the password for the default user Fixed IPFIX/NetFlow template handling in flowd component 	Changelog Billing info	



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.

NFA Documentation

Page 39 of 47



4. 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.

User profile offers this function to:

- update a user's attributes and preferences including name, email, date format, time format, etc.
- change the user's password with hints regarding password strength and confirmation mismatch.

The interface color theme can be changed here as well.

PROFILE SETTINGS	
FULL NAME:	DISPLAY DATE FORMAT:
John Smith	MM/DD/YY *
EMAIL:	DISPLAY TIME FORMAT:
admin@example.com	12 hours *
PASSWORD:	INTERFACE THEME:
Password	Light theme
CONFIRM PASSWORD:	Auto theme Dark theme
Repeat Password	Light theme

Choose between the **Light, Dark** or **Auto** options. When the Auto option is selected, NFA will follow your device's default theme.





NFA Documentation

Page 40 of 47



5. 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 or Ubuntu 20.04 LTS

Please note that NFA can also be installed on a server running CentOS 7 x86_64 Minimal – Clean Install or 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.

6. Support

Noction support team is available 24/7. Please contact our support team by emailing <u>support@noction.com</u> or by calling +1 (650) 903-7028.

7. Flow export configuration on network devices

Cisco XE:

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

- Exporter Map
 - Constant of Maria
- 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:

NFA Documentation

Page 41 of 47



```
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:

Cisco IOS:

```
flow exporter EXPORTER-1
                                           ip flow-export version 9
 destination 172.16.10.2
                                           ip flow-export destination $NFA IP 2055
 export-protocol netflow-v9
                                           interface $Interface to ISP1
 transport udp 2055
                                            ip flow ingress
 exit
                                            ip flow egress
flow record v4 r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
```

```
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
```

match transport source-port

NFA Documentation

Page 42 of 47



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;
            }
}
```

NFA Documentation

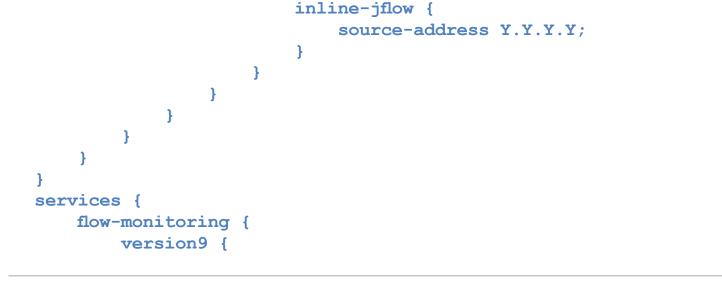
Page 43 of 47



X.X.X.X - IP address of NFA server 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;
                                  }
                              }
                         }
```



NFA Documentation

Page 44 of 47



```
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. - 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

NFA Documentation

Page 45 of 47



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

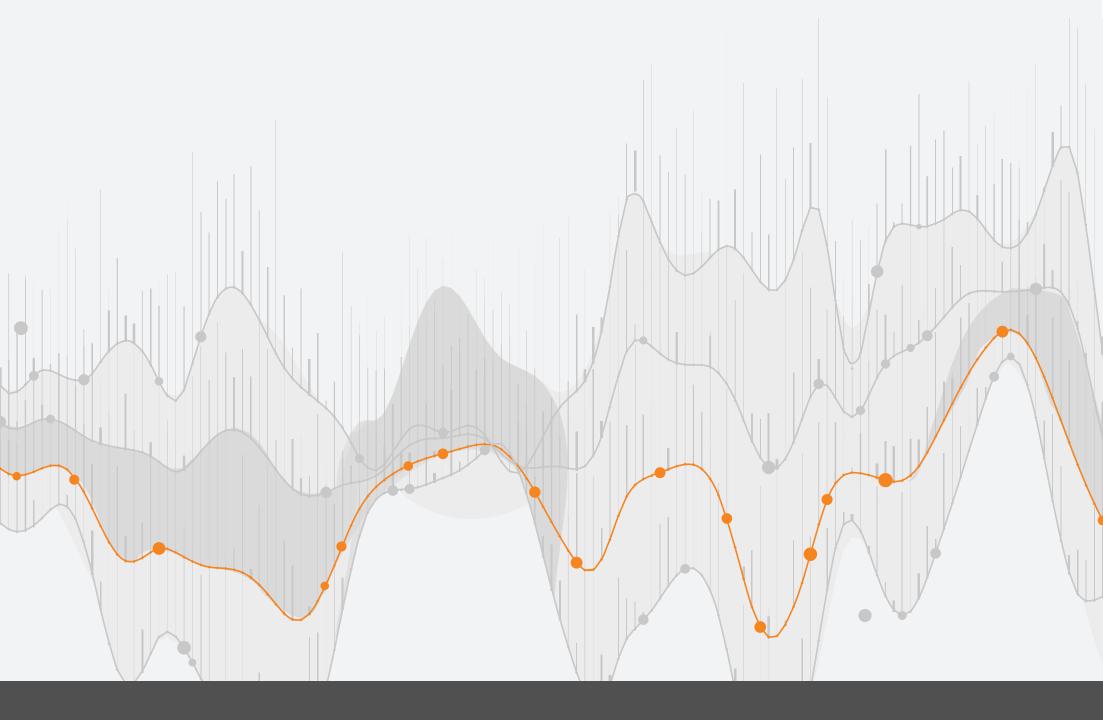
```
[Router] interface <$upstream_interface>
[Router-$upstream_interface] ip netstream inbound
[Router-$upstream_interface] ip netstream outbound
[Router-$upstream_interface] quit
```

NFA Documentation

Page 46 of 47







Noction Flow Analyzer DOCUMENTATION

Copyright ©2024 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 ©2024 Noction Inc.