Flowmon 12.1 User Guide

Introduction

The Flowmon solution comprises of Flowmon Probe, Flowmon Collector and Flowmon extension modules.

Probe Features

The Flowmon Probe is a non-invasive appliance that monitors the network IP traffic and transforms it into standard NetFlow v5/v9 or IPFIX data. This data are exported to Flowmon Monitoring Center or any third party collector for further analysis, viewing and reporting. The provided statistics are necessary for network monitoring, security, troubleshooting, IP accounting and billing, capacity planning, user and application monitoring or traffic engineering.

Although most high-end network routers support NetFlow, they often use input packet sampling and the number of supported packets/sec or flows/sec is limited, unless an additional, specialized and costly network boards are used. Furthermore, the router-based probes have fixed placement, layer 3 visibility makes them target of attacks, and the provided statistics are not reliable enough for billing or security applications. Moreover, enabling the NetFlow monitoring slows down performance of the routers.

The Flowmon Probe overcomes the limitations of router-based probes and offers standalone, L2- and L3-invisible, scalable and high-performance solution for network monitoring. It allows to generate flows statistics in environments where NetFlow exports are not available or not feasible. Typical examples are networks without NetFlow support, busy routers, L2 switches or VPNs.

The Flowmon Probe is the complete off-the-shelf appliance with easy configuration and installation. It integrates basic NetFlow data collecting, viewing and analyzing which enables quick evaluation and usage of the NetFlow technology for all – network and security operators, administrators and managers.

- High-performance standalone NetFlow v5/v9 or IPFIX probe
- Standard and hardware accelerated models
- Wire speed processing with no packet loss
- Up to 2x 100Gbps, 2x 40Gbps, 4x 10Gbps or 4x 10/100/1000 monitoring interfaces
- Compact (1U or 2U) and maintenance-free network appliance
- Non-invasive, simply plug into mirror port or TAP
- L2/L3 invisible device with IPv4, IPv6, VLAN and MPLS support
- Device can be monitored by SNMP tools (e.g. Zabbix, Nagios etc.)
- Built-in collector for quick technology evaluation
- Fully compatible with all major NetFlow collectors

Collector Features

Flowmon Collector is a stand-alone server dedicated for collection, long-term storage and analysis of NetFlow/IPFIX/sFlow statistics from Flowmon probes. For this purpose it is equipped with a huge disk capacity with RAID support. Network monitoring with multiple probes and one or more collectors is a professional solution for medium to large businesses. Flowmon Monitoring Center is used for storing and analyzing the flow data on collector. Thanks to special filters, the users are able to select particular communications based on source or destination host, used protocol, start time or many other properties acquirable by flow technology. To make the network supervision more effective, those tools also offer automatic notification and alert sending in cases of anomalies or suspicious traffic.

- High-performance collector for gathering data from multiple Flowmon Probes
- Large disk capacity enabling storing of long-term statistics
- Hardware RAID support (not available on virtual appliances)
- Best price/performance ratio in the industry
- Optimized for fast searching in statistic data
- Simple configuration via intuitive web interface

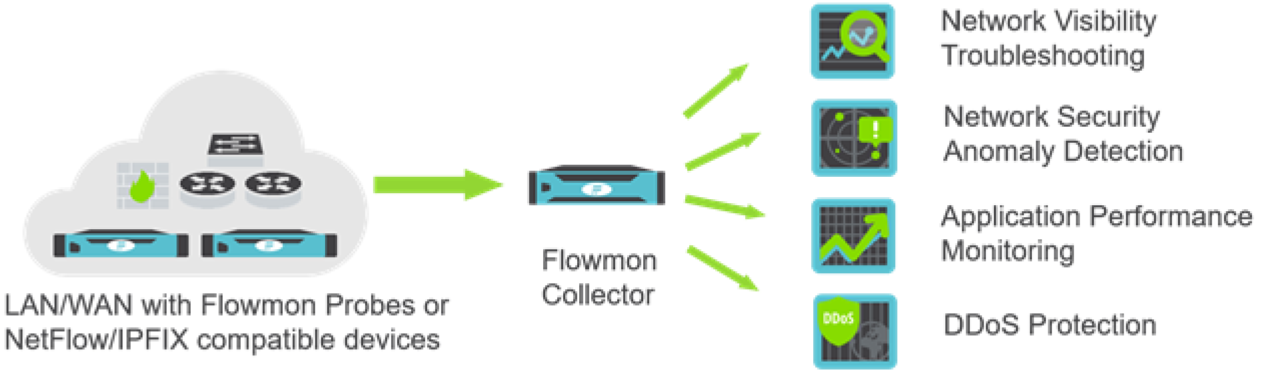
Fully compatible with all major NetFlow, IPFIX, sFlow generators (probes, routers etc.).

Flowmon Architecture

The Flowmon Probe integrates a standard or accelerated Flowmon monitoring port, Configuration Center and (if enabled by the license) Flowmon Monitoring Center. The Flowmon monitoring port captures the network traffic, computes the flow statistics and exports the NetFlow/IPFIX data. The Configuration Center enables easy remote configuration of the probe and the Flowmon Monitoring Center enables the flow data collecting (NetFlow, IPFIX, sFlow), viewing and analyzing.

The NetFlow/IPFIX data exported by the Flowmon monitoring port can be collected by the Flowmon Monitoring Center or by any other NetFlow/IPFIX collector. The Flowmon Monitoring Center comes in two versions. A built-in version is integrated into the Flowmon Probe and enables the customer to quickly evaluate the flow technology. A standalone version is implemented on the dedicated server (Flowmon Collector) and offers the professional solution for high-throughput networks.

The Flowmon Probe further supports extension modules (e.g. Flowmon ADS, Flowmon DDoS Defender, Flowmon Application Performance Monitoring etc.). See www.flowmon.com for more details about our complete Flowmon solution.


LAN/WAN with Flowmon Probes or NetFlow/IPFIX compatible devices
Flowmon Collector
Network Visibility Troubleshooting
Network Security Anomaly Detection
Application Performance Monitoring
DDoS
DDoS Protection

Flowmon Architecture

Device Description

Flowmon Probe

The Flowmon Probe is delivered as a standard 1U rack mountable server with one management port and one or more monitoring ports. The management port is used for remote configuration of the probe and for NetFlow data exports. This port should be connected to the local network. The monitoring ports are used for traffic measurement on the monitored links. All management and monitoring ports are located on the back side of the server.

The probe has a form of a common server with special software and hardware. The probe runs CentOS Linux operating system.

The front side of the server consists of an optical DVD drive, power button, USB port and LEDs for power status signalization, hard disk activity and NIC activity signalization.

The back side of the server differs for each chassis type. The chassis type can be identified by the serial number/HW ID number written in a delivery note or can be located in the Configuration Center, the Licence page, Device HWID.

Flowmon Probe Product List

Current product list including technical specifications is available at https://www.flowmon.com/en/resources?type=specification

Flowmon Collector

The Flowmon Collector is delivered as a standard 1U or 2U rack mountable server or as a virtual appliance. The collector is equipped with one management port and one export port. The management port is used for remote configuration of the collector and for reception of flow data exports via LAN. This port should be connected to the local network. The export port is connected to the network dedicated for flow export and is used for flow data reception. The collector is realized as a common server with special software and hardware. It is based on the CentOS operating system.

The front side of the server consists of an optical DVD drive, USB port, power button, RESET button and LEDs for power status signalization, hard disk activity and NIC activity signalization.

The back side of the server differs for form factor and chassis type. The chassis type can be identified by the serial number/HWID number written in a delivery note or can be located in the Flowmon Collector Configuration Center, the Licence page, Device HWID.

Flowmon Collector Product List

Current product list including technical specifications is available at https://www.flowmon.com/en/resources?type=specification

Installation and Configuration

The following chapters describe a step-by-step installation of the Flowmon appliance. If you have purchased Flowmon as a hardware appliance please continue to the chapter Web Interface. If you have purchased Flowmon as a virtual appliance, please continue with the following subchapter Installation and Configuration in Virtual Environment.

Installation and Configuration in Virtual Environment

Installation instructions for all supported virtual environments, including public clouds, can be found at https://support.kemptechnologies.com/hc/en-us/sections/4403921029645-Flowmon in *Flowmon Documentation / Flowmon Virtual Appliances & Cloud*.

Requirements

Installation and device operation doesn't require any peripherals. Usage of monitor and keyboard (or KVM) is necessary only for some service actions and for the first-time static IP configuration. The device installation requires to meet the following prerequisites:

- Available connection to the local network via standard UTP cable to connect the management port (see the section Connection to the Local Network for more details).
- Available monitored links - via the mirror/SPAN port on the router/switch or via TAP (see the section Connection to the Monitored Link - Probe only for more details).
- A computer in the local network with a web browser (Google Chrome, Mozilla Firefox, Microsoft Edge) to secure the remote access to the device. The web interface supports the latest stable versions of the aforementioned web browsers, as specified by their vendors.

Setup and Configuration

The Flowmon Probe installation consists of five steps:

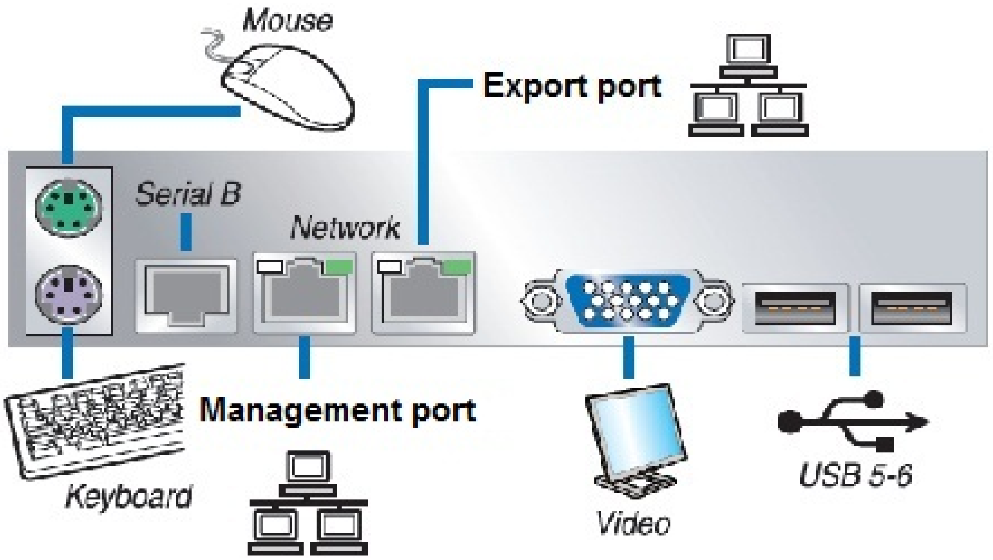
1. Mount the device to the rack (recommended).
2. Plug in the power cord.
3. Connect the management port to the local network.
4. Connect the monitored link(s).
5. Turn on the device and configure the management port IP address.

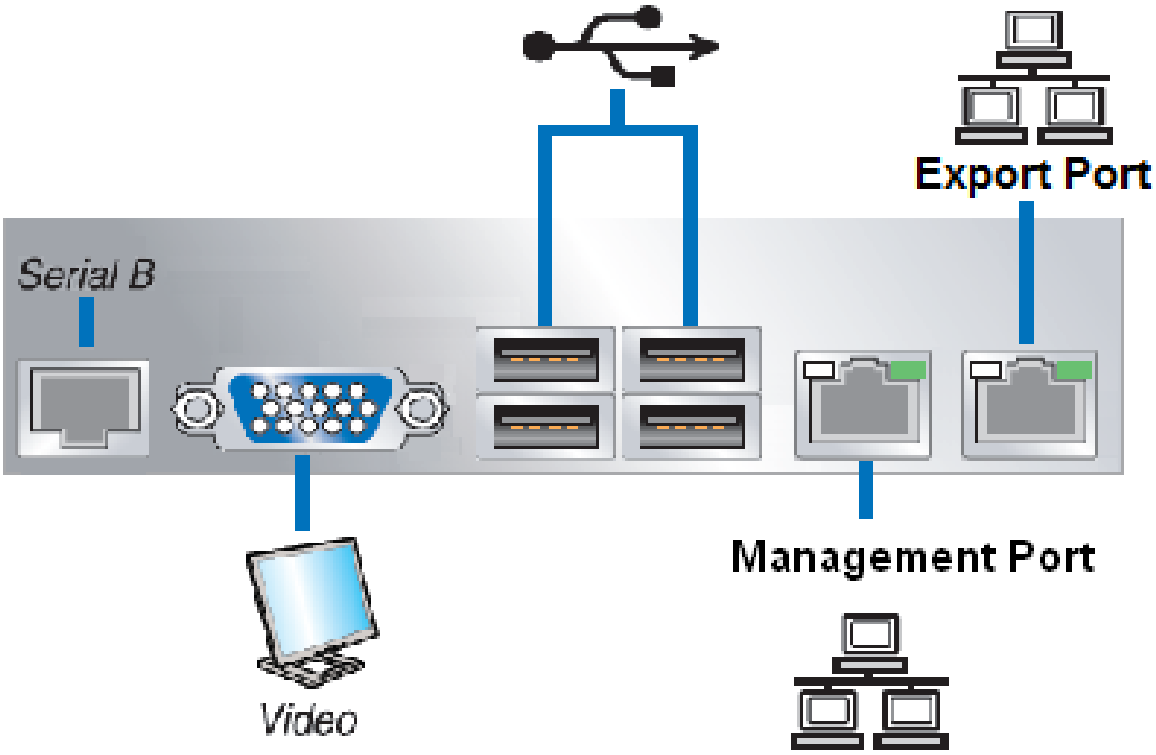
Please, complete these steps in the above-mentioned order.

Access to the device console

Flowmon may require, on some specific occasion, to perform a service task by connecting to a device console. The console can be accessed either by connecting a monitor and keyboard or via a serial link RS-

232. Connect the serial cable to the Serial RS232 connector (see the figures below). To perform a successful connection, it is necessary to configure your serial terminal in the following way: 57 600 bauds, 8 data bits, no parity, 1 stop bit and no flow control. To access the command line, enter the login **flowmon** and the password **inv3a-t3ch**.





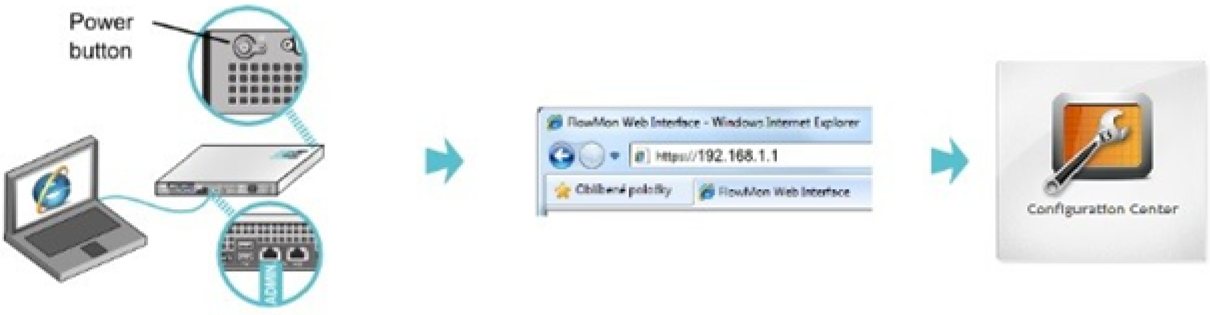
Back panel (2U model PRO)

Connection to the Local Network

The device is equipped with two management ports (RJ-45) for local network connection (doesn't apply the IFP-1000-CU - this only has one management port). Management ports are used for appliance management and for NetFlow/IPFIX data exports. For management port connection, please u se common UTP cables . Ethernet 10/100/1000 is supported. The IP address of the management port can be configured in two ways - using the web GUI or using the console.

IP address configuration using the web GUI

Connect your computer to the administration interface (see figure below) using the Ethernet cable. Set your computer up with a static IP address 192.168.1.10 and mask 255.255.255.0. Start a web browser and enter IP address 192.168.1.1.

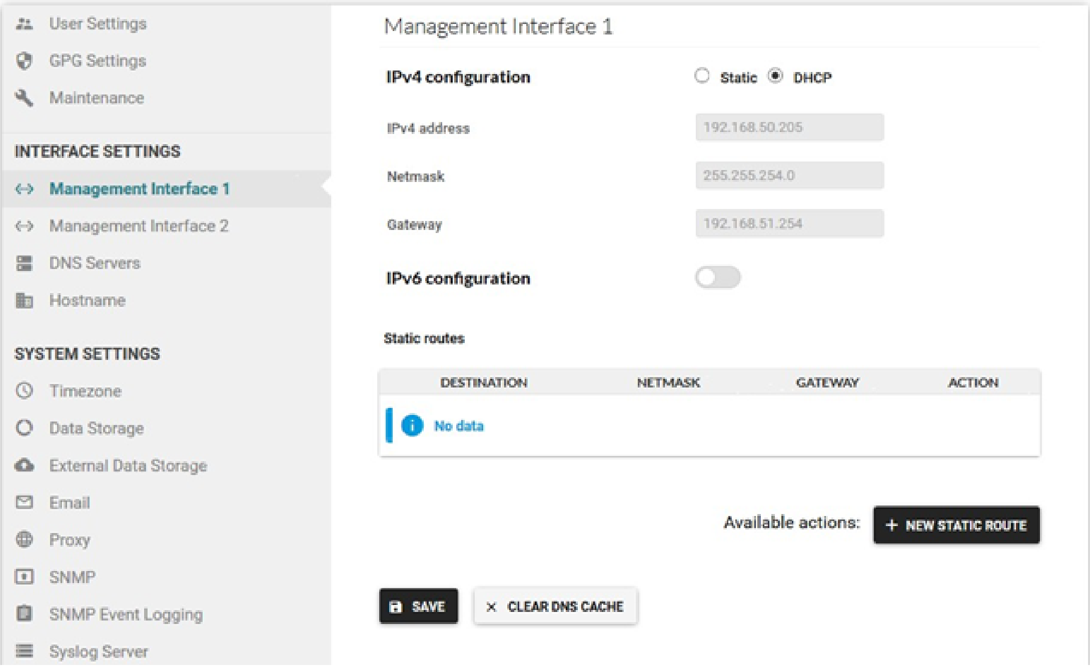


Device GUI connection

Click the **Configuration Center** button and enter the user login **admin** and password **admin**. Navigate to the **System** page, the **Interface Settings** section, **Management Interface 1** and perform the IP address configuration (see the figure Management IP configuration with GUI).

After configuration of an IP address and clicking the **Save** button, the device will be unavailable due to the IP address change. Wait approximately 10 seconds, disconnect it from the computer and connect the management interface to your LAN network. If you configured the IP address to be set up by DHCP, press the power button shortly and wait until the device turns off. Then turn on the device again. After a few minutes, it acquires the IP address from the DHCP protocol. If you have configured the IP address statically, you don't need to turn off the device.

Now, check the connection to your device. If it stays unavailable, check your network configuration (look at your routers whether the path to your device is correctly set up etc.). If you are still not available to connect to the device, please repeat the IP address configuration using a **sysconfig** application (see the following section IP address configuration using console).



Management Interface 1

IPv4 configuration ○ Static ● DHCP

IPv4 address: 192.168.50.205

Netmask: 255.255.254.0

Gateway: 192.168.51.254

IPv6 configuration

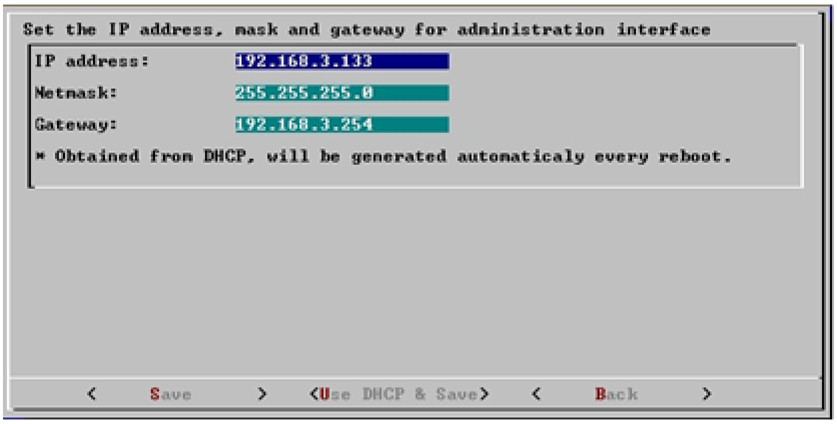
Static routes

DESTINATION	NETMASK	GATEWAY	ACTION
No data			

Management IP configuration with GUI

IP address configuration using console

Connect to the device console (see the section Access to the device console) and run the **sysconfig** application. In the application menu, choose the **Management port** item, enter the proper values and press the **Save** button if you want to configure the IP address statically. If you want to use DHCP, press the **Use DHCP & Save** button. Then see the console output to check if the IP configuration was performed successfully.



```
Set the IP address, mask and gateway for administration interface
IP address:           192.168.3.133
Netmask:              255.255.255.0
Gateway:              192.168.3.254
* Obtained from DHCP, will be generated automaticaly every reboot.

      <    Save      >   <Use DHCP & Save>   <     Back     >
```

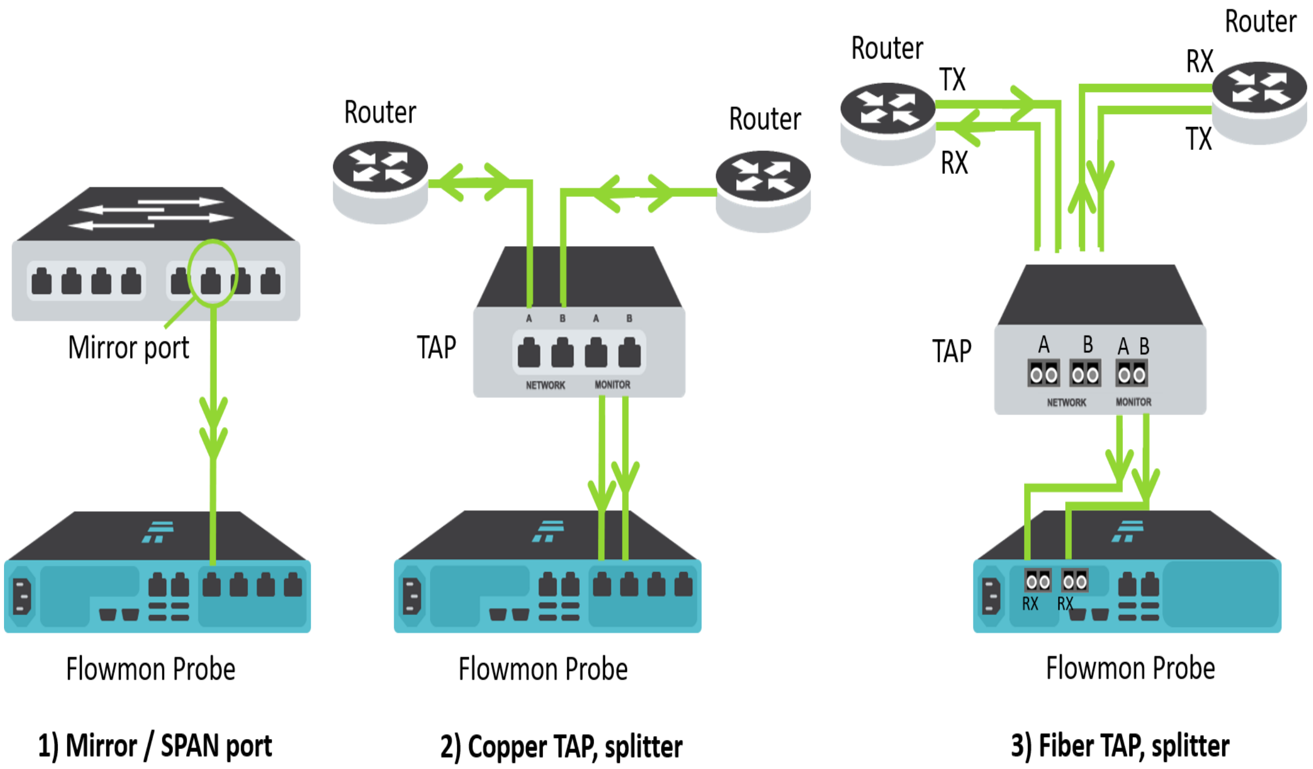
Management IP configuration with sysconfig application

Connection to the Monitored Link - Probe only

The location of the probe and connection point of the monitoring interface should be determined by the network administrator. The Flowmon Probe is mostly used to monitor the traffic on central network switches/routers, on the output and input points of the network, critical points (data storage, server farms), saturated links, firewalls or VPN access points. To connect the monitoring interface, use appropriate network cables according to the link speed and used medium. Flowmon probes support both, copper or fiber medium and they are able to monitor multiple fully saturated links up to 10 Gbps.

The probe installation is easy and straightforward. There are several ways how to connect your probe into the existing infrastructure with minimal need to change anything in it. The probe monitoring interfaces can be connected in two ways:

1. using the mirror port of router or switch (SPAN port)
2. connect directly to the monitored link via Ethernet TAP or splitter



1) Mirror / SPAN port

2) Copper TAP, splitter

3) Fiber TAP, splitter

Connection of the Flowmon Probe monitoring interfaces

The connection using the mirror port is shown in the figure Connection of the Flowmon Probe monitoring interfaces - 1) Mirror / SPAN port. This solution is completely non-invasive and only requires to configure the particular router or switch to mirror demanded traffic. This solution brings the best benefits, if the switch or router is able to mirror multiple interfaces. This enables the probe to monitor all the traffic passing through the router/switch. Disadvantage of this approach comes from the limits of the mirroring appliance as the amount of mirrored data can exceed the mirroring link capacity and cause data sampling to degrade the results of probe monitoring.

The best monitoring results on a saturated link can be achieved using Ethernet TAP or splitter. TAP is passive, high-reliable appliance able to replicate full-duplex traffic into two monitoring ports. It is simply inserted into the monitored link having no influence on the passing data. This situation is shown in the figure Connection of the Flowmon Probe monitoring interfaces - 2) Copper TAP, splitter and 3) Fiber TAP, splitter. The main advantage of this approach is that it can be used in any point of your network and the point can be easily changed according to your needs. The monitored link stays uninterrupted even in case of the TAP power failure or probe malfunction.

Turning on the Device

Turn on the device by pressing the turn on/off button on the front side. The LED above/behind the button will light up. Please, wait approximately 2 minutes until the device starts. The proper function can be verified by accessing the web interface of the device using a web browser. Use the IP address configured in the section Connection to the Local Network . If the main page of the device web interface will appear, the device installation is successfully finished. To log in, use a default user name “admin” and password “admin”. Please, change the login password as soon as possible to avoid an unauthorized access (see the section User and Roles Settings).

Recommended Post-Installation Steps

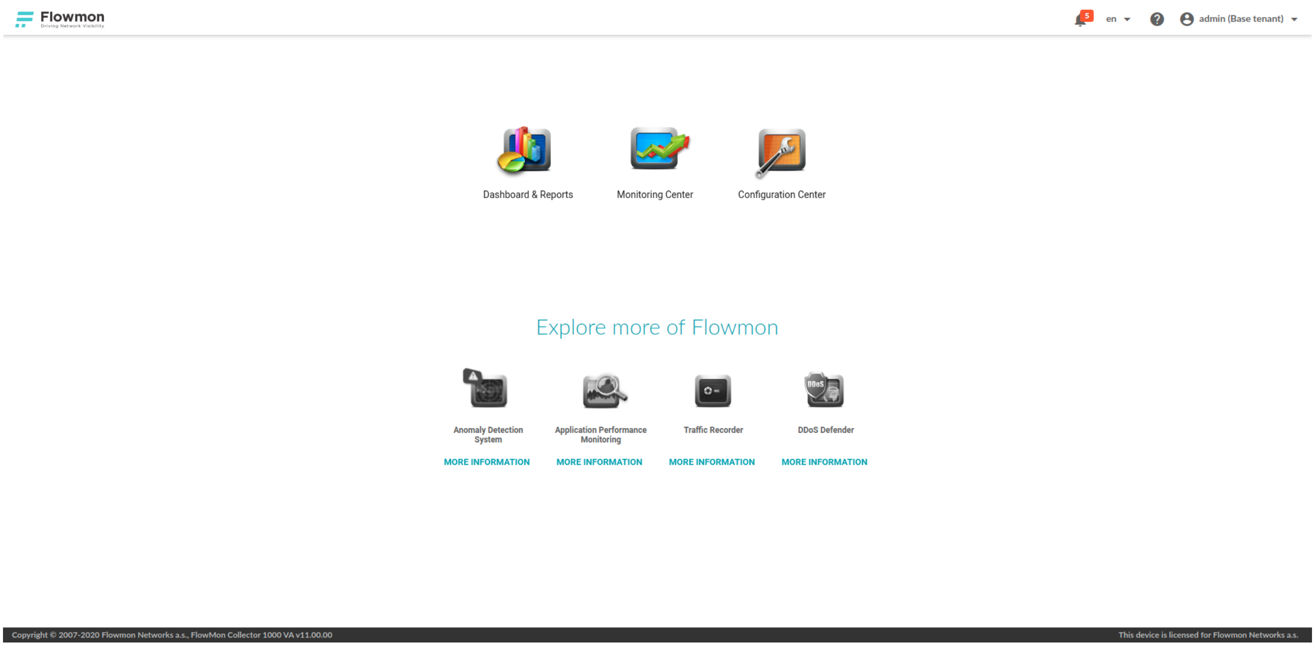
1. Change the default login name and password for the SSH access. Login to the device console (see chapter Access to the device console) and change the password for user flowmon by the application **sysconfig**.
2. Change the default password for web interface access. Login to the Configuration Center and follow the instructions in the section User and Roles Settings.
3. If you have changed a hostname of your device, it is advisable to generate a new SSL Certificate. Please, follow the steps in the section Maintenance.
4. Set your timezone and NTP server in the Configuration Center (see the section Timezone) to adjust the time on your probe.
5. **Probe only:** In the default configuration, the probe exports NetFlow data on its built-in collector. If you wish to export data to a professional NetFlow collector (e.g. Flowmon Collector), change the monitoring port settings following the instructions in the section Monitoring ports. Note: the built-in collector is limited by lack of disk space, slow hard disk operations and lower CPU and memory performance in comparison to a specialized NetFlow collector. For achieving the best performance, we recommend to use a professional standalone NetFlow collector (e.g. Flowmon Collector).
6. If you use SNMP for supervising your network appliances, configure the SNMP daemon running on the probe. Please, follow the instructions in the section SNMP Daemon.
7. Initialize a built-in collector database by its deleting. **This step will irreversibly delete all data in the database!** Perform this step only after the first start of the collector or if you want to delete the database. Please, follow the instructions in the Built-In Collector section.

Web Interface

The Flowmon device configuration is performed using the web interface. The same interface is used to access the built-in collector and other add-on modules. Start a supported web browser and enter the device's IP address or domain name. For the first login use default user name "admin" and password "admin".

ⓘ **Note**

The FMC (built-in collector) is defaultly enabled and generated NetFlow data is sent to this collector. For a long-time monitoring purposes, dedicated collector is a recommended solution (e.g. Flowmon Collector).



Copyright © 2007-2020 Flowmon Networks a.s., FlowMon Collector 1000 VA v11.00.00

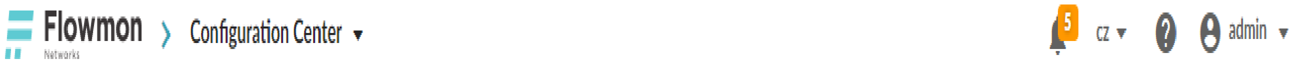
This device is licensed for Flowmon Networks a.s.

Note

The web interface can be extended with other optional modules.

The Configuration Center (FCC) allows you to remotely setup your device. The Flowmon Monitoring Center (FMC) is used to observe and analyze collected NetFlow data. Detailed description of both centers can be found in the sections Configuration Center and Flowmon Monitoring Center.

Page header contains important elements. In the upper left corner there is the Flowmon Networks logo. Clicking on it will redirect you to the main page, from which you can access all active modules. If you are logged in a module, its name is shown in the box displayed next to the logo. You can click on it to open a list of other module icons to quick skip to another module GUI.



On the right side there is a status icon (bell). When everything is working correctly, the icon is grey. If there are some warnings or errors, it shows the number of messages in red. Click on the icon to open a window listing all messages, time and severity. Users in the admin group can delete these messages.

The second icon displays abbreviation of the currently selected language. To change the language, click the icon and select a new one.

Click the third icon with a question mark to show a menu with user guide and a link to a feedback page (you can report bugs, errors or leave feedback here).

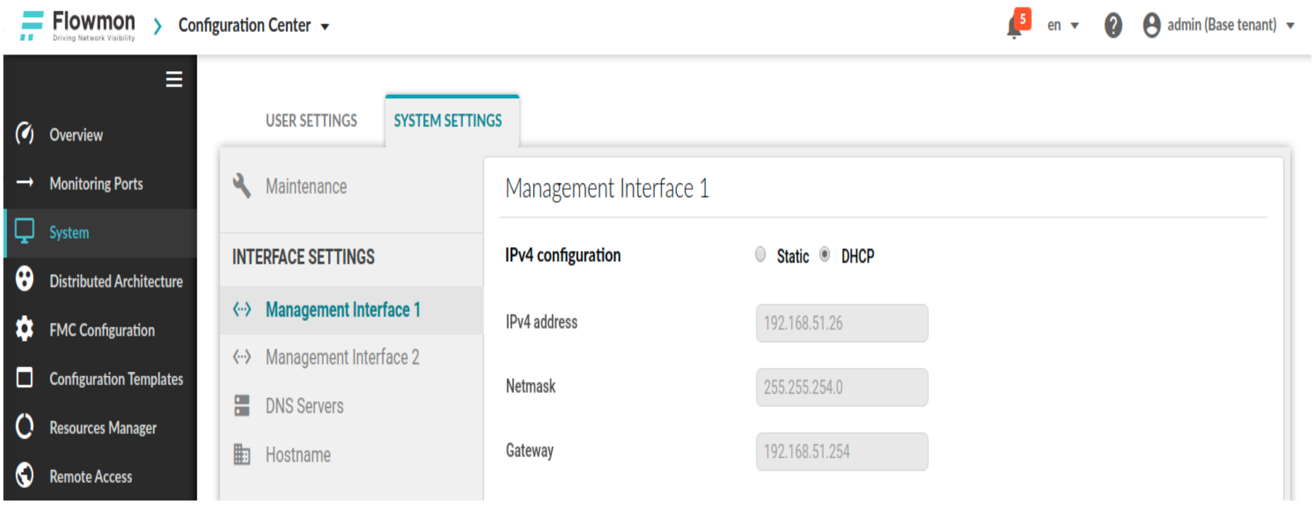
The last box shows the currently logged user and active tenant name. Click on the user name to open a drop-down menu. Click on the gear icon to open a **User settings** form. You can change active tenant under the **Tenant** option (for more information about tenants see Tenants). There is also an option to log out.

Configuration Center

The Flowmon Collector parameters and behavior can be configured via the Configuration Center (FCC). The access to FCC is realized via a secured HTTPS protocol. The following sections describe functions and options of FCC. On the left side of the page you can see a main menu including items **Overview**, **System**, **Disk Management**, **Quota Manager**, **Remote Access**, **Logs**, **Version** and **License**. Another items may appear in the menu as well (e.g. **Monitoring ports**), depending on license. The company logo in the top left corner is used as a link to the main page of the web interface. The Disk Management page is available for non-PRO models only (i.e. collectors with SW RAID).

System

This page provides the basic device settings, which should be configured at the first login. Especially it is advisable to change the login and password for particular modules, set the NTP server and configure settings of the management interface.



Management Interface 1

IPv4 configuration ○ Static ● DHCP

IPv4 address 192.168.51.26

Netmask 255.255.254.0

Gateway 192.168.51.254

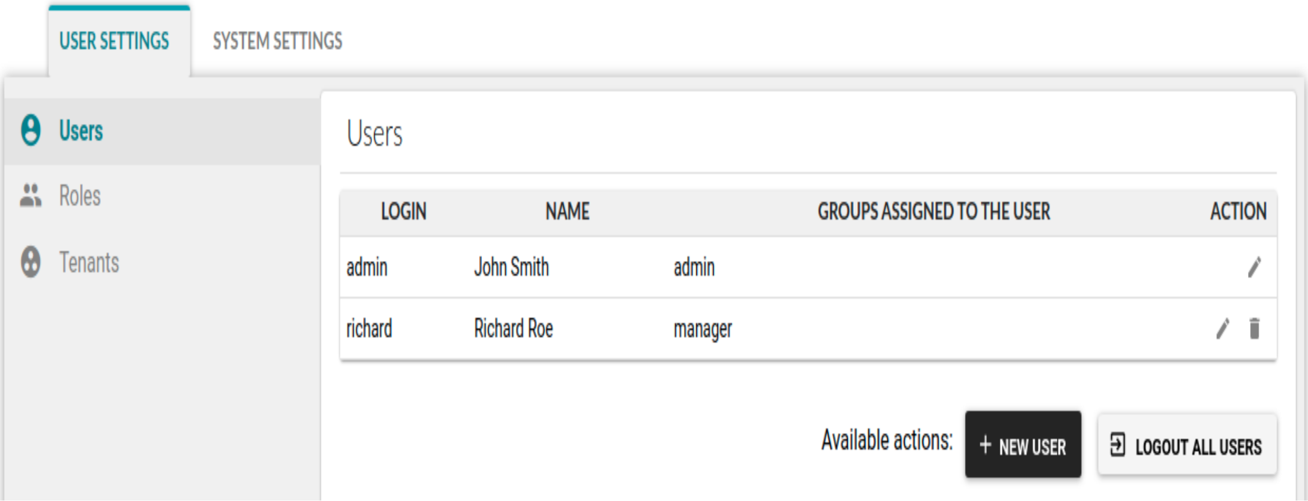
User Settings

The user settings is maintained in the following sections:

- Users
- Roles
- Tenants

Users

This page serves for configuration of user accounts. You can define users who can access Flowmon Configuration Center or other installed modules. It's recommended to change default user name and password on the first login.



USER SETTINGS SYSTEM SETTINGS

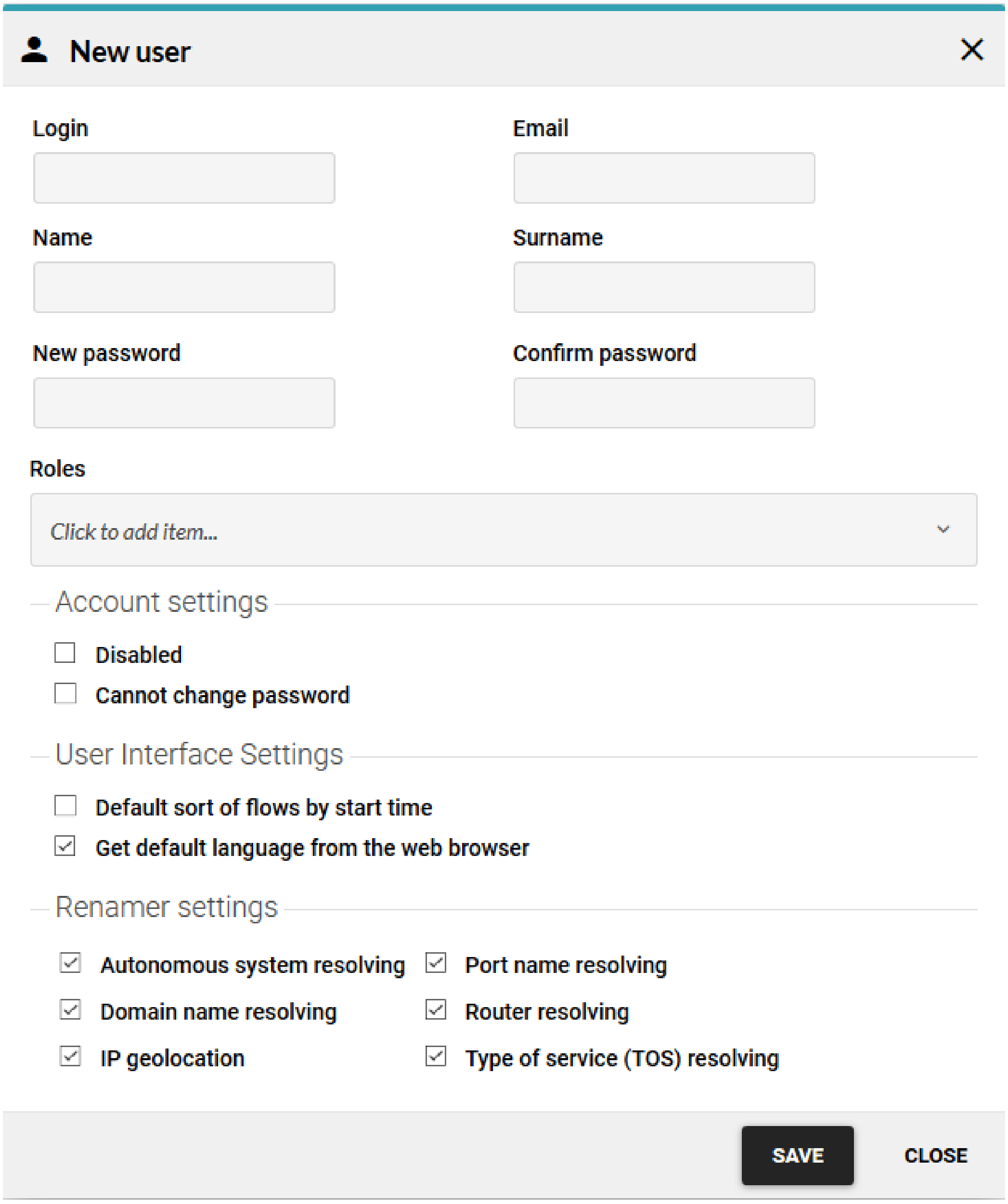
Users
Roles
Tenants

Users

LOGIN	NAME	GROUPS ASSIGNED TO THE USER	ACTION
admin	John Smith	admin	✎
richard	Richard Roe	manager	✎ 🗑

Available actions: + NEW USER | LOGOUT ALL USERS

Press the **New user** button and fill in user data and their roles in the pop-up window. A user personal settings can be defined here. If the user should not be able to change their password or if they should be temporarily denied access to the system, check appropriate checkboxes. You will be informed if any input is not correct. In Renamer Settings, resolvable items can be enabled or disabled for automatic resolving or translation. To save your changes, press the **Save** button.



New user ✕

Login

Email

Name

Surname

New password

Confirm password

Roles

Click to add item...

Account settings

☐ Disabled

☐ Cannot change password

User Interface Settings

☐ Default sort of flows by start time

☑ Get default language from the web browser

Renamer settings

☑ Autonomous system resolving ☑ Port name resolving

☑ Domain name resolving ☑ Router resolving

☑ IP geolocation ☑ Type of service (TOS) resolving

SAVE CLOSE

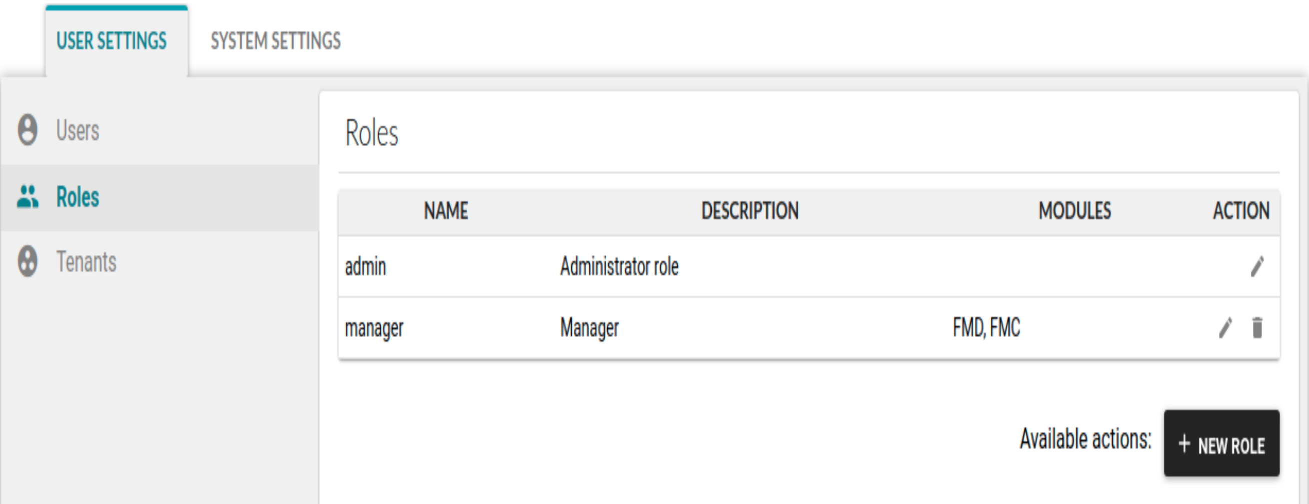
Create new user form

If you want to change an existing user, click the **Edit** button. An edit form will pop up. To save changes, press the **Save** button. User can be removed by clicking the **Delete** button. Deleting of user admin is not allowed and this login cannot be changed.

ⓘ **Note**
In case you forgot the admin password you can reset it by the following step. Login to the CLI and run a command ./restore_factory_settings.sh. Script will ask you few questions. For question Do you want to reset GUI admin password [y/N]? answer y. The password will be reset to admin.

Roles

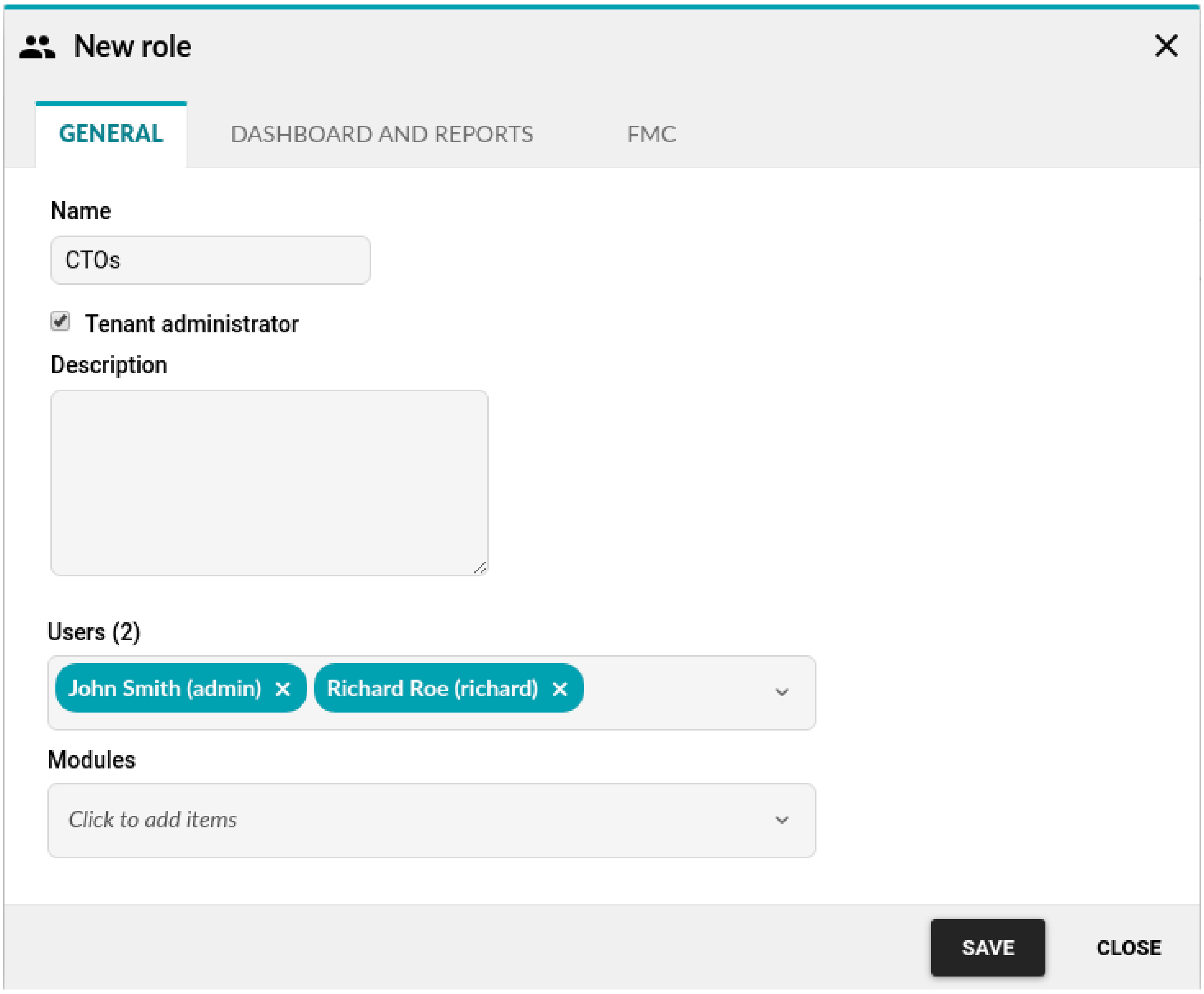
This page serves for configuration of roles.



Roles

NAME	DESCRIPTION	MODULES	ACTION
admin	Administrator role		✎
manager	Manager	FMD, FMC	✎ 🗑

Press the **New role** button to open a form for new role. In this form, you can assign this role to users and configure access to specific modules. Access to **Configuration center** module is available only for users with **Tenant administrator** role. Some modules have their own permission to be set, this configuration will be available in special tabs in this form. You can find more info in particular module chapters.



Name: CTOs

☑ Tenant administrator

Description

Users (2): John Smith (admin) ✕ Richard Roe (richard) ✕

Modules: Click to add items

Migration of former roles

When updating to Flowmon 11, all roles with access to Configuration center module will become **Tenant administrators** on the base tenant.

Access to the tenants is managed by roles. There are three types of roles in a context of a tenant management:

- **Super admin**
  - Tenant administrator on the base tenant
  - User with this role can switch to all tenants.
  - Access to configuration center is not restricted.
- **Tenant administrator of other than base tenant**
  - Capability of this role is restricted to a home tenant and its children only.
  - Configuration center is limited only to subtenants management, presets and logs.
- **Tenant user**
  - No tenant administrator role.
  - User has access only to his home tenant.
  - Access to the configuration center is not allowed.

Tenants

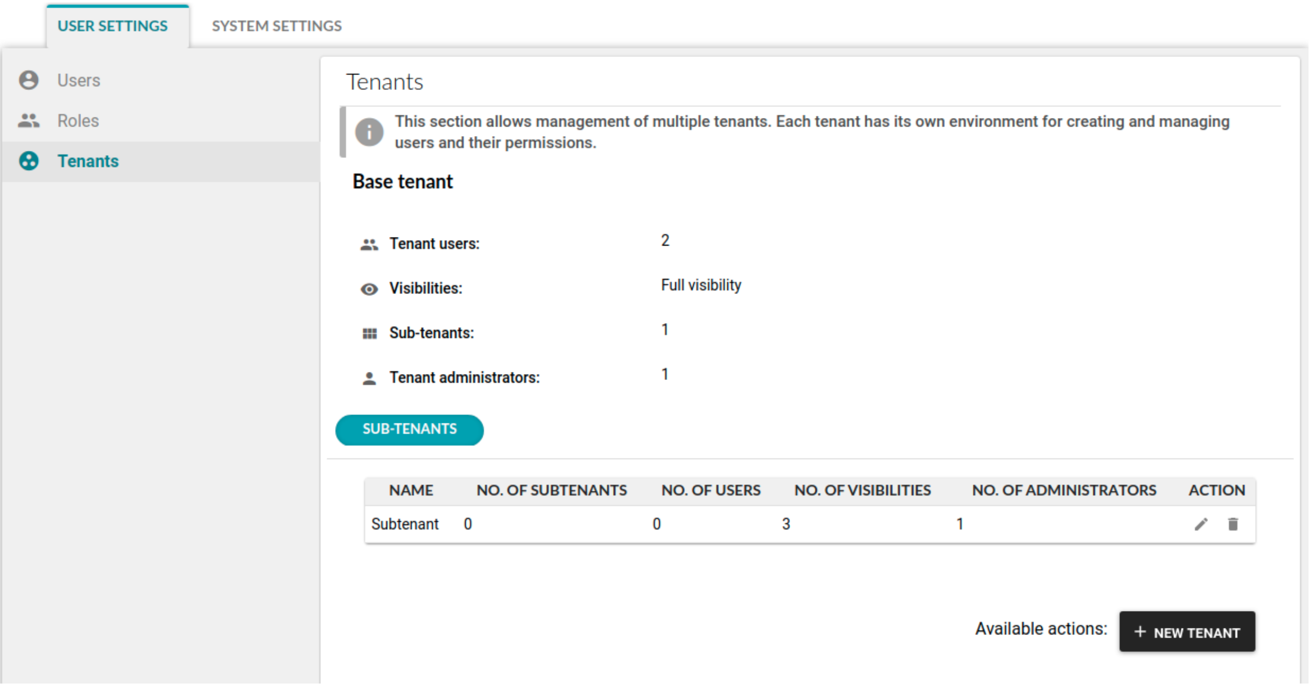
Flowmon allows you to run a multi-tenant environment.

Tenant is an isolated environment for creating and managing users and their permissions. Each user and role are defined in a single tenant. By default, all current permissions are defined in the **Base tenant**.

Please notice that you can still use Flowmon in single tenant mode and that you are not required to create any new subtenants.

Tenant administrator can create multiple **tenants** defined by **flow sources** and **profiles** visible for particular tenant. **Tenant administrator** can also manage users and roles within the tenant - assign **visibilities** on flow sources to users and roles. **Tenant administrator** can assign subset of flow sources and profiles according to tenant definition.

Tenant overview page



Tenants

This section allows management of multiple tenants. Each tenant has its own environment for creating and managing users and their permissions.

Base tenant

Tenant users:	2
Visibilities:	Full visibility
Sub-tenants:	1
Tenant administrators:	1

NAME	NO. OF SUBTENANTS	NO. OF USERS	NO. OF VISIBILITIES	NO. OF ADMINISTRATORS	ACTION
Subtenant	0	0	3	1	

Available actions:

The Tenant overview page is divided into two parts. The upper part displays the **current tenant summary** whereas the bottom part displays the **subtenants structure** and **current tenant visibility** details.

Current tenant summary

Tenant users represent number of users created in this tenant.

Visibilities show how many sources and profiles are assigned to this tenant. Base tenant has **full visibility** - access to data of profiles and source is not restricted on this level. Visible profiles and sources can be restricted to users also by role definition (see Role Access Permissions for more information).

Sub-tenants represent number of tenant created in this tenant.

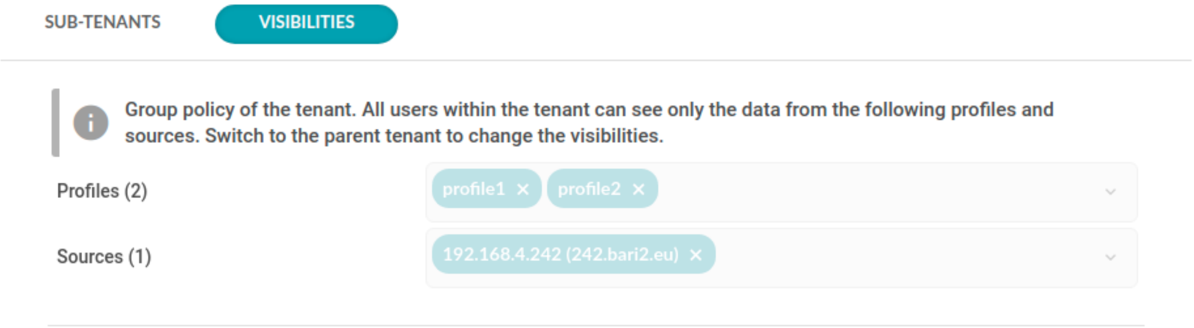
Tenant administrators represent number of users with tenant administration role for this tenant.

Sub-tenants structure tab

This tab lists direct sub-tenants of the current tenant.

Current tenant visibilities tab

You can see active subtenant's visibilities in the **Visibilities** tab (this tab is hidden in the base tenant, because of the full visibility).



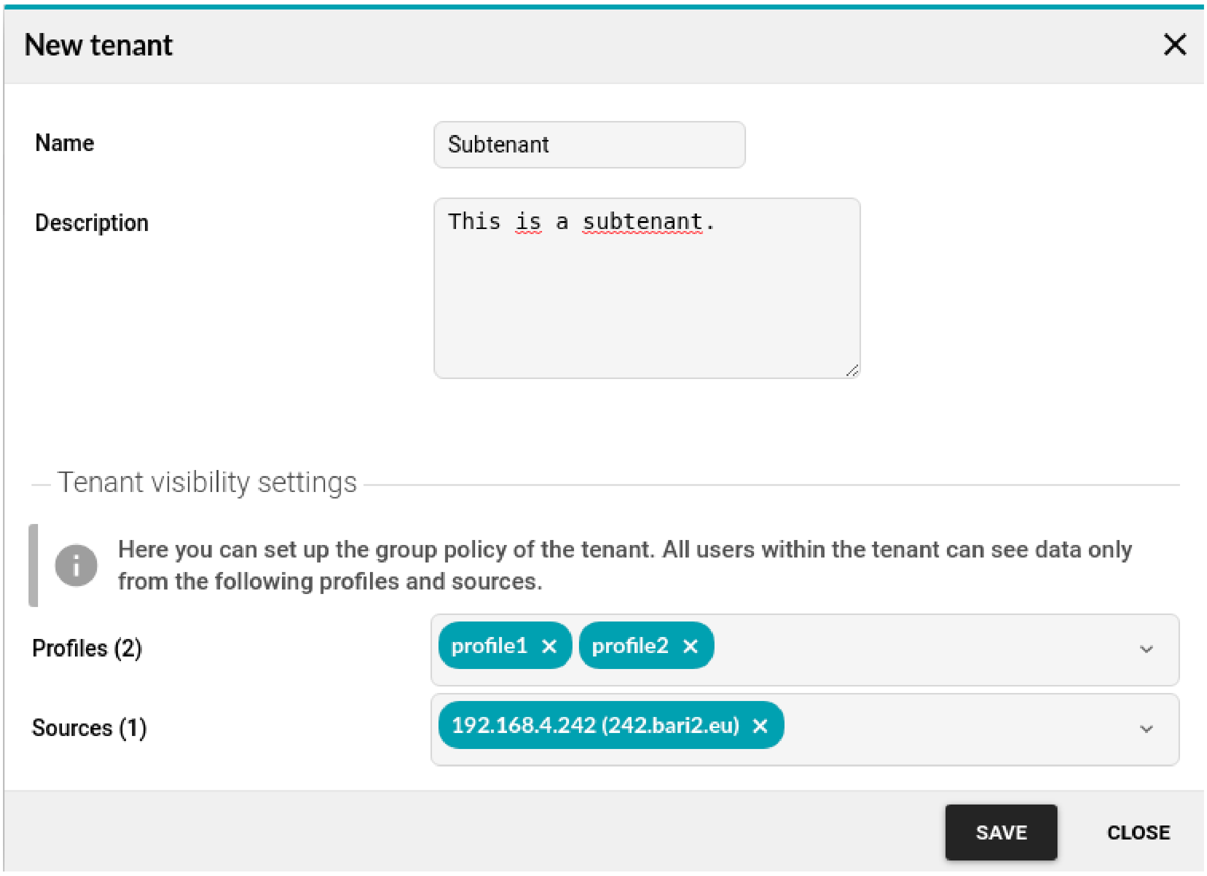
Group policy of the tenant. All users within the tenant can see only the data from the following profiles and sources. Switch to the parent tenant to change the visibilities.

Profiles (2): profile1 ×, profile2 ×

Sources (1): 192.168.4.242 (242.bari2.eu) ×

Creating/Updating a Tenant

Press the **New tenant** button to create a new subtenant. Fill in a tenant name, description and specify visibility settings. All users within the tenant can see data only from profiles and sources specified here. To save your changes, press the **Save** button. You can create tenants up to the two levels of nesting (base tenant > level 1 subtenant > level 2 subtenant). In the base tenant you can create tenants of a first level of an nesting. To create tenants of a second level of nesting, switch to a subtenant in which you want to create this tenant.


New tenant

Name: Subtenant

Description: This is a subtenant.

Tenant visibility settings

Here you can set up the group policy of the tenant. All users within the tenant can see data only from the following profiles and sources.

Profiles (2): profile1 ×, profile2 ×

Sources (1): 192.168.4.242 (242.bari2.eu) ×

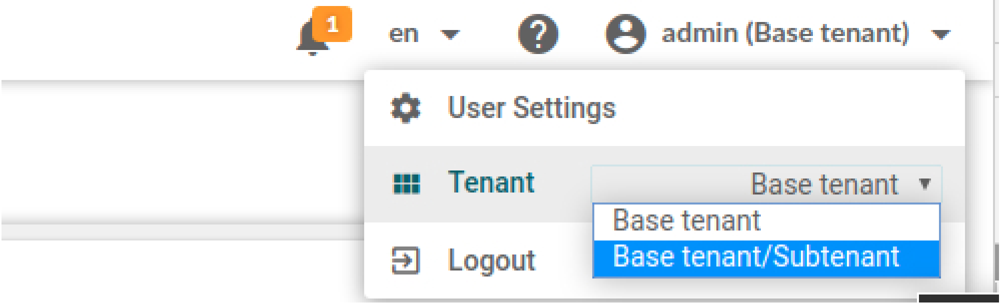
If you want to edit an existing tenant, click the **Edit** button. An edit form will pop up. To save changes, press the **Save** button. Tenant can be deleted by clicking the **Delete** button. Base tenant deletion is not allowed and its visibilities cannot be changed.

Warning

Deleting tenant will lead to deletion of all users, roles, profiles, alerts, reports, schedules and subtenants created in this tenant! All deleted settings will be logged in FCC - Logs.

Changing active tenant

Active tenant name is displayed next to the name of currently logged user. To change the active tenant, select the user name. Drop-down menu will appear. Select the active tenant name and choose tenant from drop-down with all available tenants (see Roles for more information about tenant accessibility).



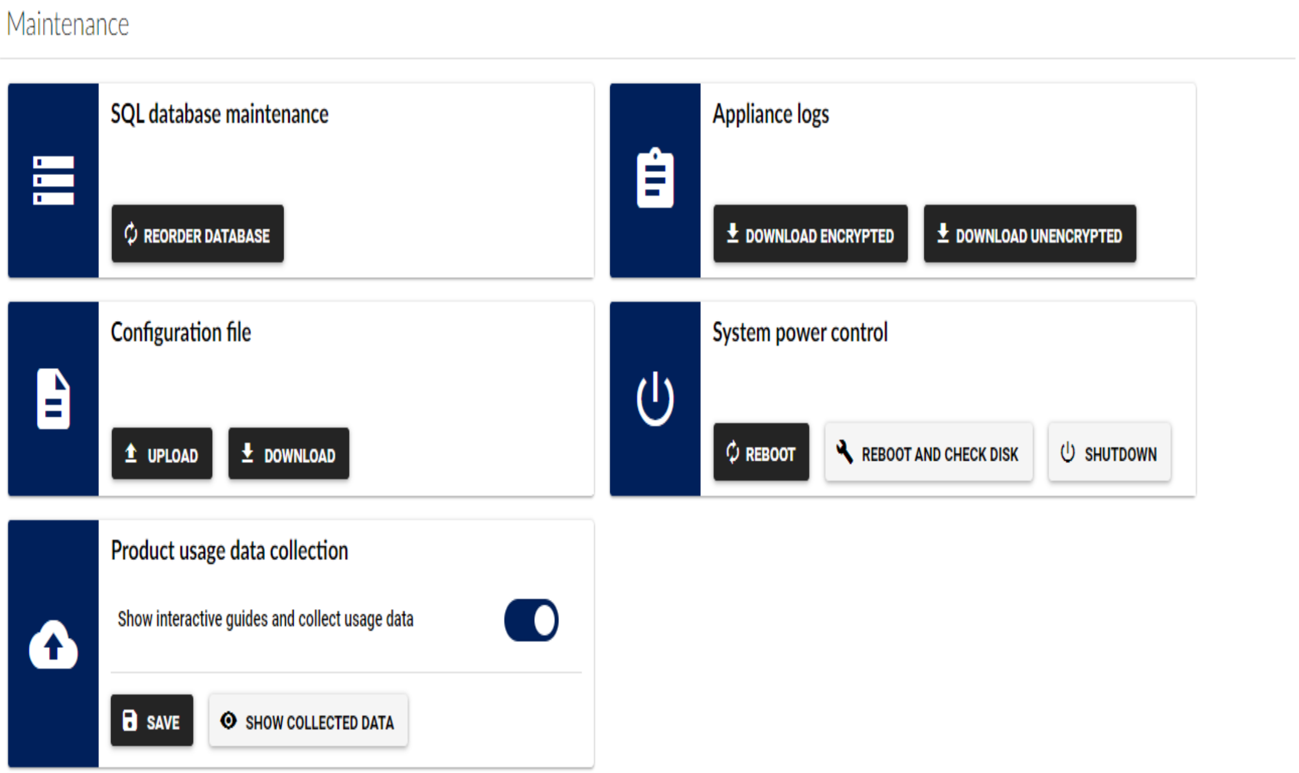
Maintenance

This page serves as a guidepost for the maintenance of your appliance. It provides tools for configuration management, log retrieval, database maintenance and power control.

- SQL database maintenance
- Appliance logs
- Configuration file
- System power control
- Product usage data collection

SQL database maintenance

The device is running an SQL database, which is used by many Flowmon modules. This database is reordered in regular manner to achieve its fast response. In some cases, when a huge amount of records is stored to database in a short time (e.g. restoring from backup), the regular reordering process is not enough to keep all the SQL records in an optimal status. If the response of Flowmon modules which use the SQL database is getting slower as a result of unordered data, it is necessary to perform a full reorder process. This process needs an exclusive access to the database, and therefore to lock it for writing. For this reason, some Flowmon modules could not work properly; please wait until the reorder process is completely finished. To run the full reorder process, press the **Reorder database** button.



Appliance logs

Logs contain service information. In case of system faults or improper behavior of system, please download and send these logs to support@flowmon.com

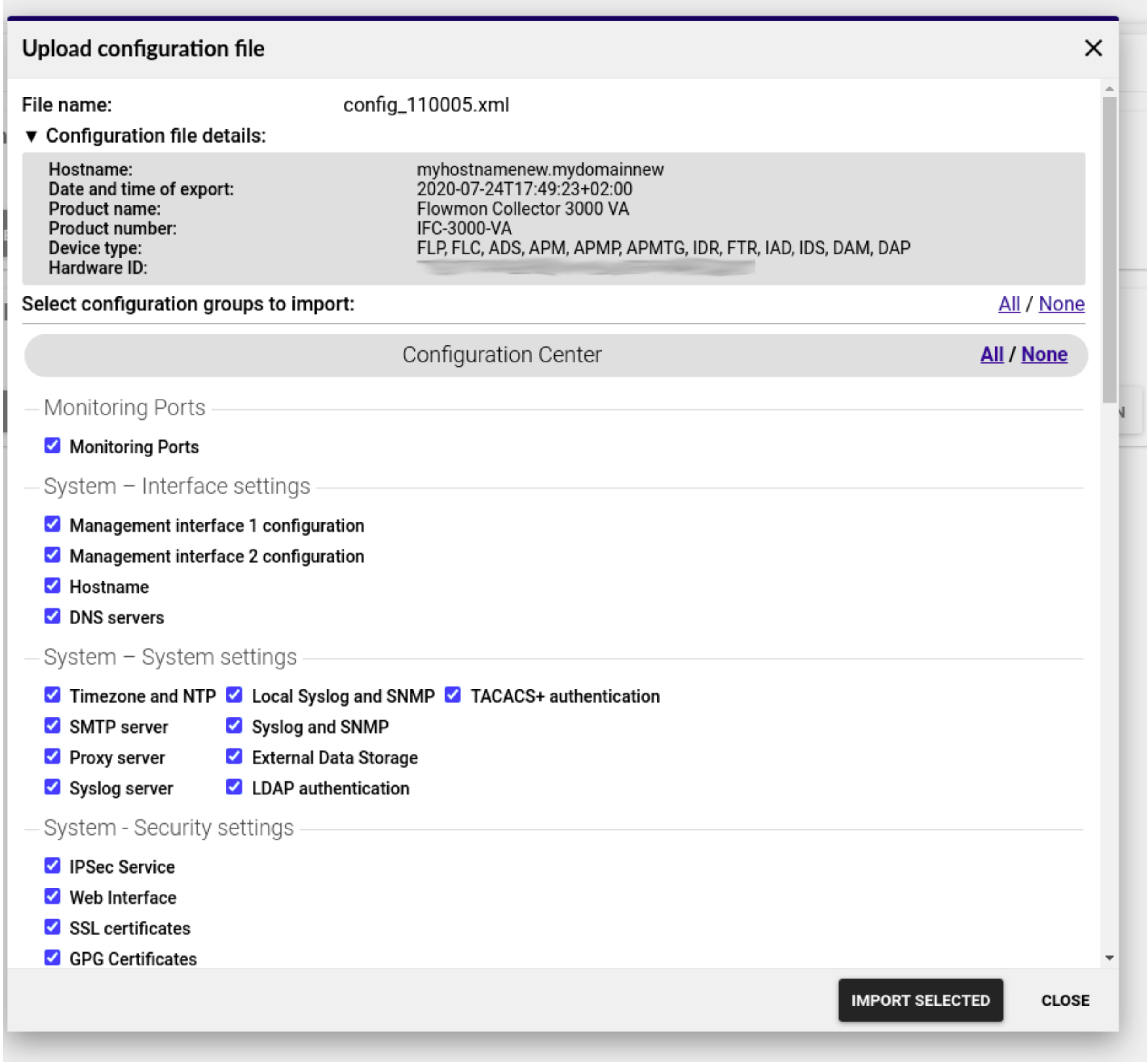
Configuration file

Configuration file can be stored as an XML file and this file can be used as a backup in case of loosing the configuration or for distribution of configuration to other devices. Click on the **Download** button to display a form for selection of the configuration groups you want to store. After applying this form, the XML file with configuration is generated and the browser asks you to store it on your computer.

To restore the previously saved configuration, click on the **Upload** button. In the dialog box, select the XML file with configuration. After the upload, the form is shown where you can select which configuration groups stored in the XML you want to apply. For configuration import, only values that are understandable for the target device will be applied. In Additional Settings, the import mode can be selected. The mode **Add and modify** is non-destructive and only adds those elements which are not present in target system and are present in XML file (e.g. Profiles). Elements which are already present in the target system are modified only according to the settings in XML file; the captured are not modified. Elements which are present in the target system and are not present in XML are left untouched. On the other hand, the mode **Delete and create** is destructive and causes e.g. wiping of all captured data in profiles (if the configuration group Profiles is selected). This mode completely remove all old elements at first (don't care whether they are present in XML file or not) and then creates new elements from XML. Thus, this mode is suitable especially for cleaning the device.

Forward compatibility of exported configuration is guaranteed throughout all releases with the same major version number. Between major versions, the last stable release of the previous major version is guaranteed to export configuration that is compatible with the next major version. Example: For Flowmon 11 releases, configuration export from any 11.0.x release is compatible with any 11.1.y release. For upgrades between major versions, if 10.3.9 is the last version released for Flowmon 10 then configuration exported from this version is compatible with Flowmon 11 and can be imported.

The import process can take even several minutes depending on the selected configuration groups. Once the import is finished, the status window is shown with result of import of each selected configuration group.



Upload configuration file

File name: config_110005.xml

▼ Configuration file details:

Hostname:	myhostnamenew.mydomainnew
Date and time of export:	2020-07-24T17:49:23+02:00
Product name:	Flowmon Collector 3000 VA
Product number:	IFC-3000-VA
Device type:	FLP, FLC, ADS, APM, APMP, APMTG, IDR, FTR, IAD, IDS, DAM, DAP
Hardware ID:	[redacted]

Select configuration groups to import: All / None

Configuration Center All / None

Monitoring Ports

☑ Monitoring Ports

System – Interface settings

☑ Management interface 1 configuration
☑ Management interface 2 configuration
☑ Hostname
☑ DNS servers

System – System settings

☑ Timezone and NTP
☑ SMTP server
☑ Proxy server
☑ Syslog server
☑ Local Syslog and SNMP
☑ Syslog and SNMP
☑ External Data Storage
☑ LDAP authentication
☑ TACACS+ authentication

System - Security settings

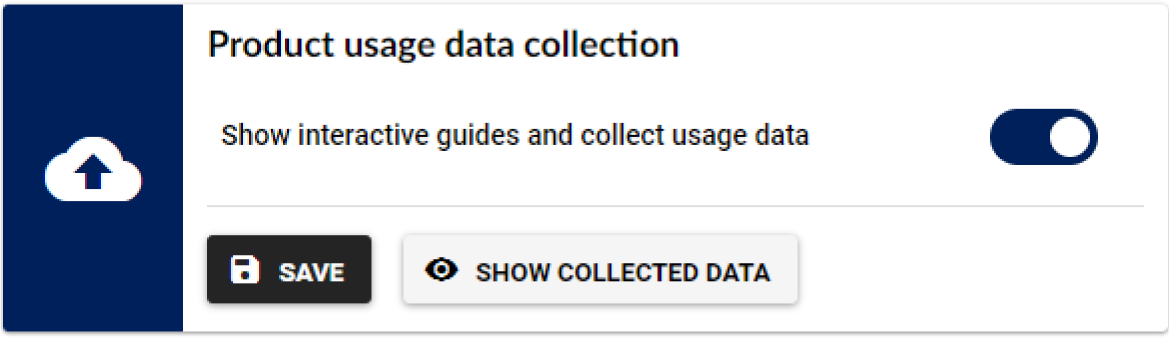
☑ IPSec Service
☑ Web Interface
☑ SSL certificates
☑ GPG Certificates

System power control

Use these options to remotely reboot or shutdown your device. To restart the device, press the **Reboot** button and confirm your action. To bring the device down in a secure way, press the **Shutdown** button and confirm your action. Please note that the device cannot be remotely powered on.

Product usage data collection

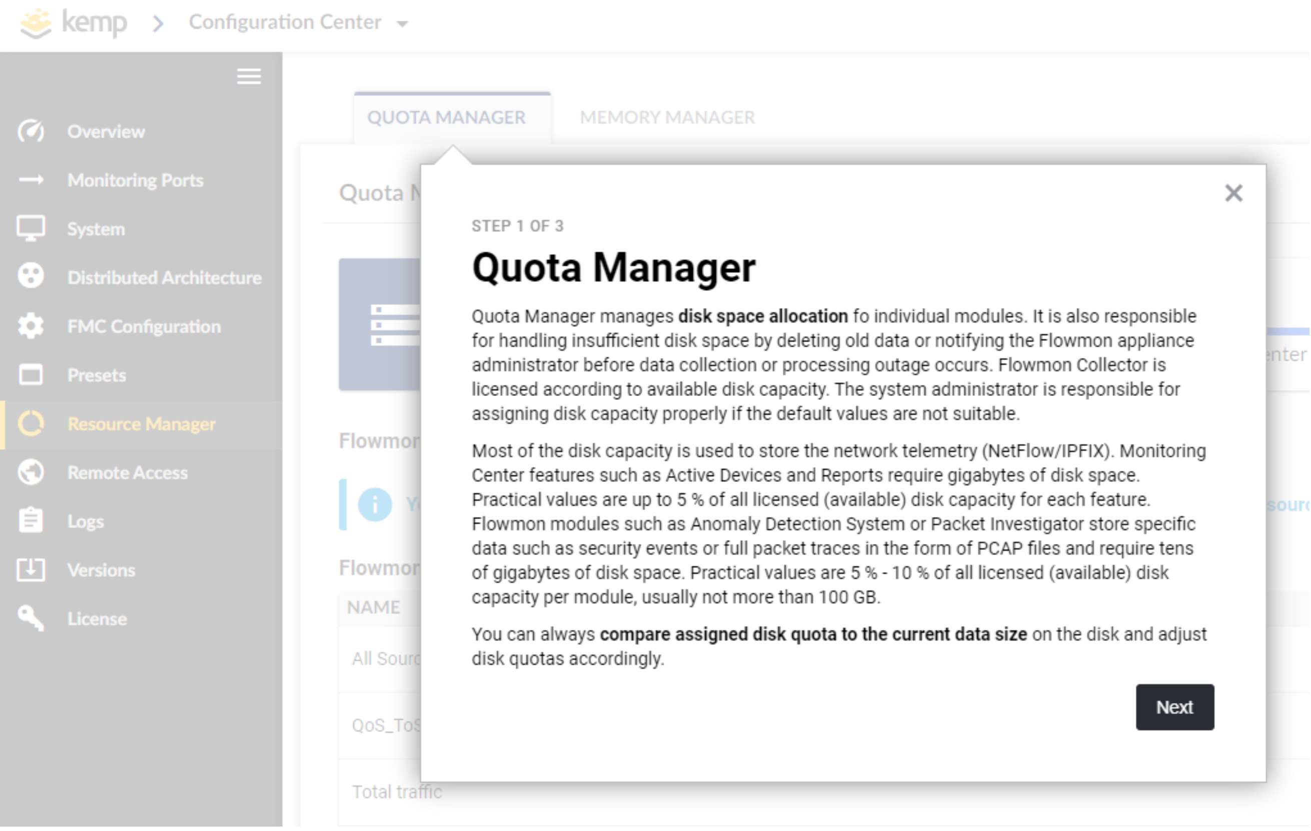
Options in this section control interactive, in-product user guides and usage data collection. These two features are inextricably linked and can only be enabled/disabled together. Use the slider to turn features on/off and click on the **Save** button to apply the change. Both are enabled by default on all appliances and require client's connectivity to public Internet to communicate with external servers that provide guide content and collect usage data.



Product usage data collection

Show interactive guides and collect usage data

Interactive, in-product guides provide brief description for key features of the product along with useful advice on how to use them correctly. Each guide tied to a specific section of the UI is displayed only once to every user. Once a guide has been displayed to a user, it will not be shown again. The display status of all guides, for all users, can be reset by the appliance administrator by using the CLI-based factory reset tool and choosing ONLY the " Do you want to reset interactive guides? " option. Initially, guides will cover key features in Configuration Center, new guides will be added over time.



STEP 1 OF 3

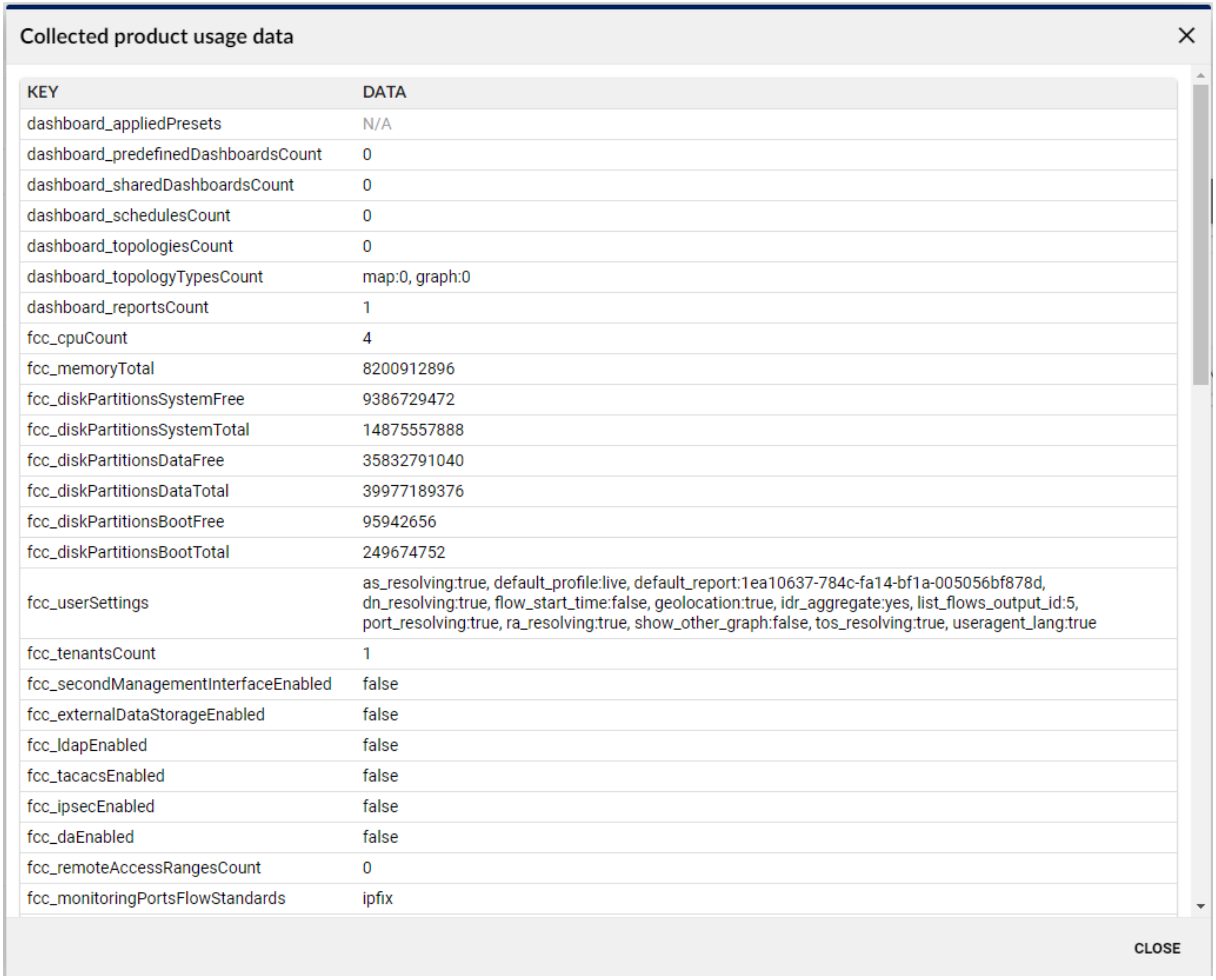
Quota Manager

Quota Manager manages **disk space allocation** fo individual modules. It is also responsible for handling insufficient disk space by deleting old data or notifying the Flowmon appliance administrator before data collection or processing outage occurs. Flowmon Collector is licensed according to available disk capacity. The system administrator is responsible for assigning disk capacity properly if the default values are not suitable.

Most of the disk capacity is used to store the network telemetry (NetFlow/IPFIX). Monitoring Center features such as Active Devices and Reports require gigabytes of disk space. Practical values are up to 5 % of all licensed (available) disk capacity for each feature. Flowmon modules such as Anomaly Detection System or Packet Investigator store specific data such as security events or full packet traces in the form of PCAP files and require tens of gigabytes of disk space. Practical values are 5 % - 10 % of all licensed (available) disk capacity per module, usually not more than 100 GB.

You can always **compare assigned disk quota to the current data size** on the disk and adjust disk quotas accordingly.

In an effort to improve the product, **product usage data collection** collects solely non-personally identifiable data about the appliance configuration; including usage statistics, enabled features, and general configuration. It does NOT collect customer data stored on or processed by Flowmon appliances. To display and review collected data, click on the **Show collected data** button.



Collected product usage data

KEY	DATA
dashboard_appliedPresets	N/A
dashboard_predefinedDashboardsCount	0
dashboard_sharedDashboardsCount	0
dashboard_schedulesCount	0
dashboard_topologiesCount	0
dashboard_topologyTypesCount	map:0, graph:0
dashboard_reportsCount	1
fcc_cpuCount	4
fcc_memoryTotal	8200912896
fcc_diskPartitionsSystemFree	9386729472
fcc_diskPartitionsSystemTotal	14875557888
fcc_diskPartitionsDataFree	35832791040
fcc_diskPartitionsDataTotal	39977189376
fcc_diskPartitionsBootFree	95942656
fcc_diskPartitionsBootTotal	249674752
fcc_userSettings	as_resolving:true, default_profile:live, default_report:1ea10637-784c-fa14-bf1a-005056bf878d, dn_resolving:true, flow_start_time:false, geolocation:true, idr_aggregate:yes, list_flows_output_id:5, port_resolving:true, ra_resolving:true, show_other_graph:false, tos_resolving:true, useragent_lang:true
fcc_tenantsCount	1
fcc_secondManagementInterfaceEnabled	false
fcc_externalDataStorageEnabled	false
fcc_ldapEnabled	false
fcc_tacacsEnabled	false
fcc_ipsecEnabled	false
fcc_daEnabled	false
fcc_remoteAccessRangesCount	0
fcc_monitoringPortsFlowStandards	ipfix

When enabled, this feature sends collected data to external servers via a secure communication channel.

Interface Settings

The interface settings is maintained in the following sections:

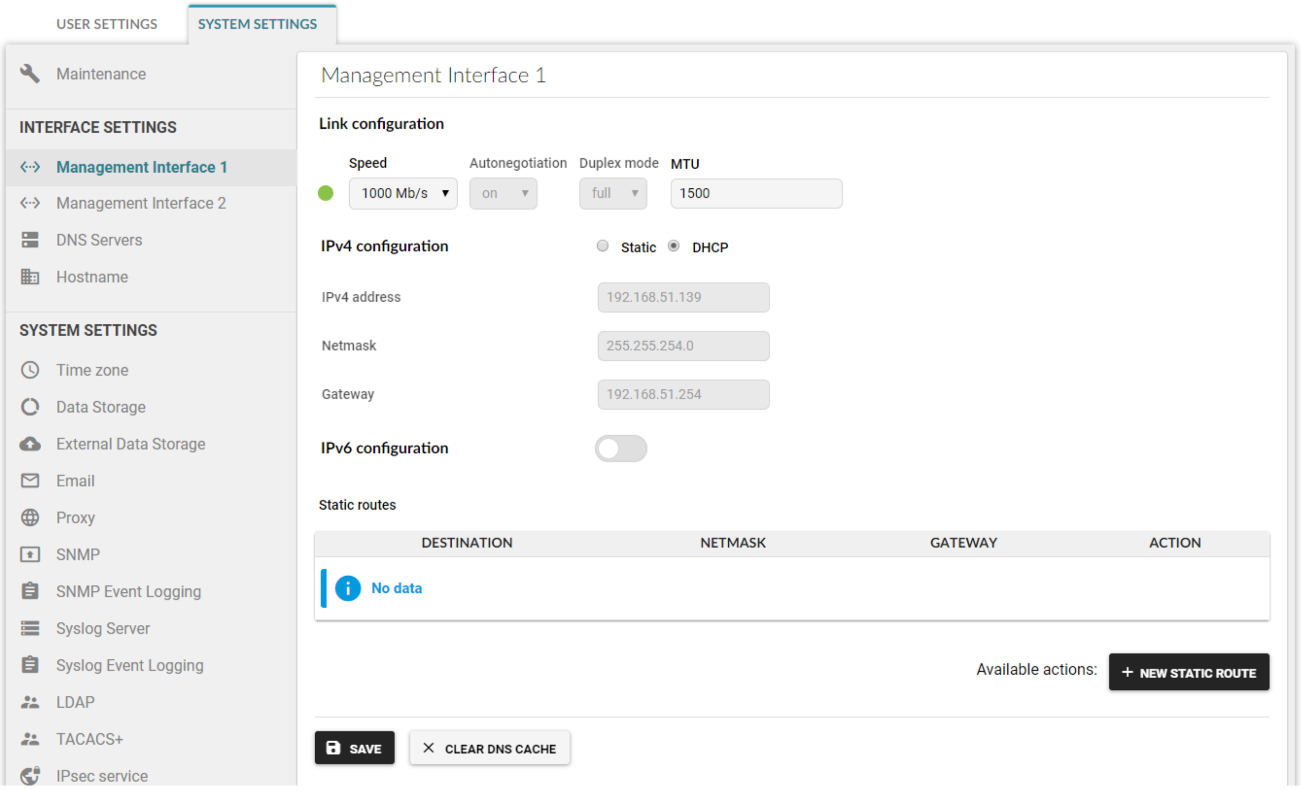
- Management Interface 1
- Management Interface 2
- DNS Servers
- Hostname

Management Interface 1

The **Management Interface 1** is used for configuration of management network interface no. 1.

Attention

When you assign an invalid IP address, the web interface will become unreachable! In this case it is necessary to log in to the device locally and fix the settings using the **sysconfig** tool.



Management Interface 1

Link configuration

Speed	Autonegotiation	Duplex mode	MTU
1000 Mb/s	on	full	1500

IPv4 configuration ○ Static ● DHCP

IPv4 address: 192.168.51.139

Netmask: 255.255.254.0

Gateway: 192.168.51.254

IPv6 configuration: off

Static routes

DESTINATION	NETMASK	GATEWAY	ACTION
No data			

Available actions: + NEW STATIC ROUTE

SAVE · CLEAR DNS CACHE

The first part of the table is used for configuration of IP address and for setting the default gateway. These data can be assigned either statically by choosing the **Static** button and filling the respective fields or dynamically by choosing the **DHCP** button and rebooting the device. IPv6 address, prefix and gateway can be assigned as well when the **IPv6 configuration** toggle switch is checked.

The **Clear DNS cache** button is used for clearing the DNS cache - all DNS names will require to be resolved again from DNS server.

The **New static route** button opens a form where you can add a static route. Edit existing static routes by clicking the edit button (pencil icon) and remove it by clicking on the delete button (garbage can icon).

To apply your changes, click the **Save** button

Management Interface 2

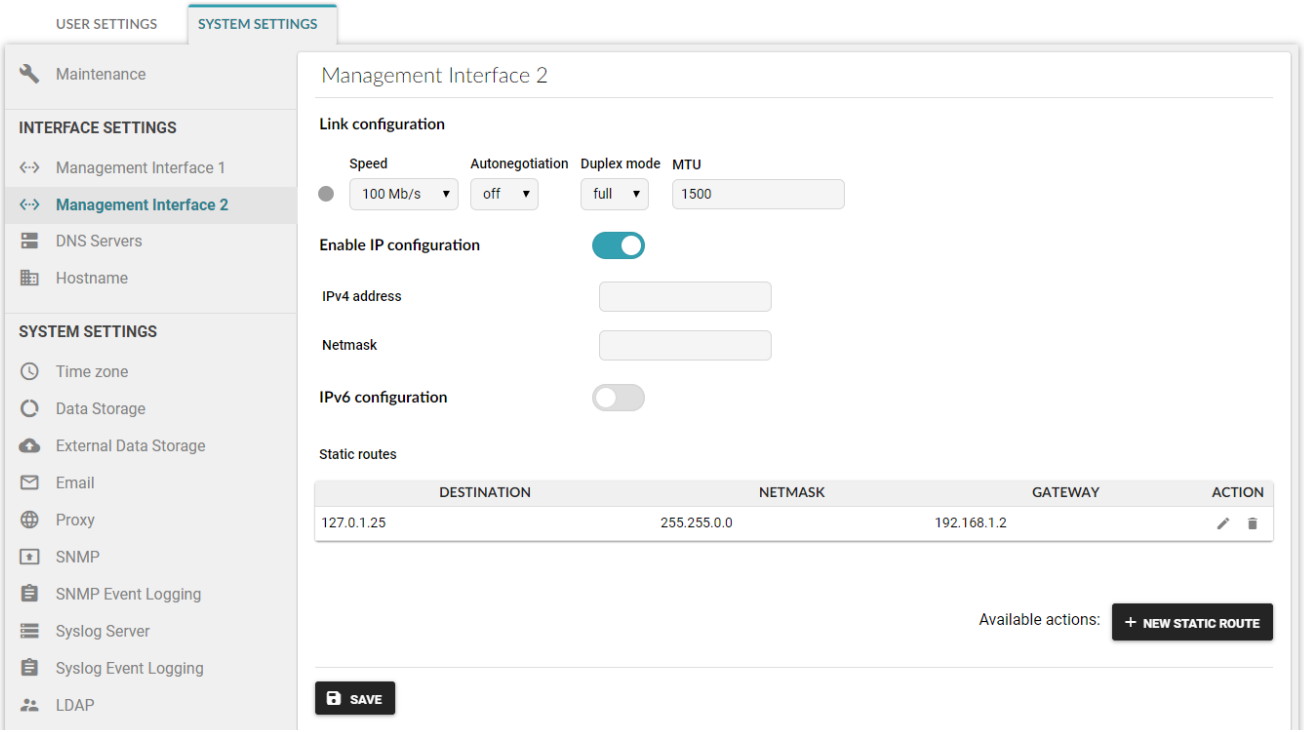
The **Management Interface 2** is used for configuration of management network interface no. 2. It can be assigned a static IP address only.

Attention

When you assign an invalid IP address, the web interface will become unreachable! In this case it is necessary to log in to the device locally and fix the settings using the **sysconfig** tool.

The **New static route** button opens a form where you can add a static route. Edit existing static routes by clicking the edit button (pencil icon) and remove it by clicking on the delete button (garbage can icon).

To apply your changes, click the **Save** button.



Management Interface 2

Link configuration

	Speed	Autonegotiation	Duplex mode	MTU
●	100 Mb/s ▾	off ▾	full ▾	1500

Enable IP configuration: on

IPv4 address:

Netmask:

IPv6 configuration: off

Static routes

DESTINATION	NETMASK	GATEWAY	ACTION
127.0.1.25	255.255.0.0	192.168.1.2	✎ 🗑

Available actions: + NEW STATIC ROUTE

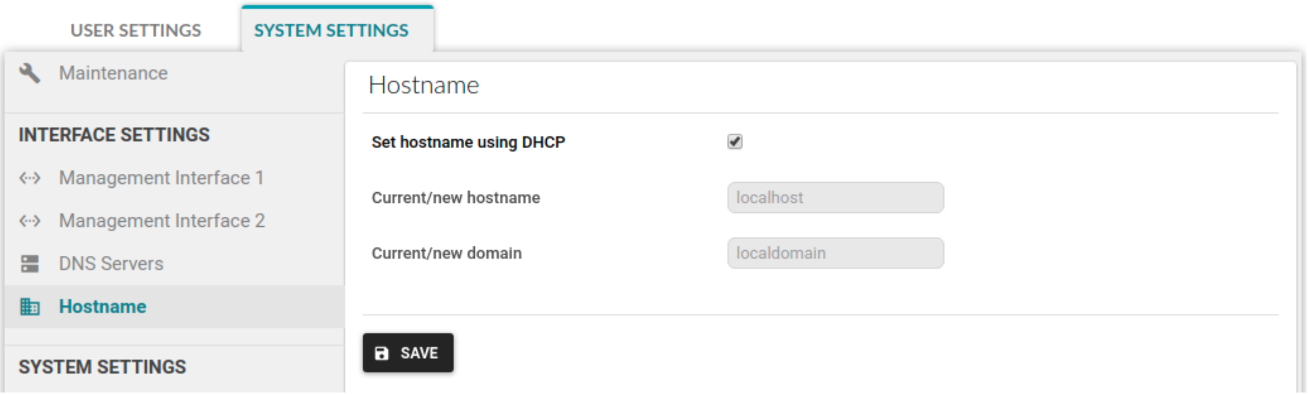
SAVE

DNS Servers

Configuration of IP addresses of the Primary and Secondary DNS server.

Hostname

This page is used for configuration of hostname and domain of the device. The hostname can be set either automatically by DHCP (requires a properly configured DHCP and DNS server), or it can be set manually. To assign the values automatically, check the **Set hostname by DHCP** checkbox. Manual assignment can be done by unchecking the checkbox and entering the hostname to the **Hostname** field and domain to the **Domain** field. To apply your changes, press the **Save** button.



Hostname

Set hostname using DHCP ☑

Current/new hostname: localhost

Current/new domain: localdomain

SAVE

System Settings

The system settings is maintained in the following sections:

- Timezone
- External Data Storage
- Data Storage (on a virtual platform)

- Email
- Proxy
- SNMP
- SNMP Event Logging
- Syslog Server
- Syslog Event Logging
- LDAP
- TACACS+

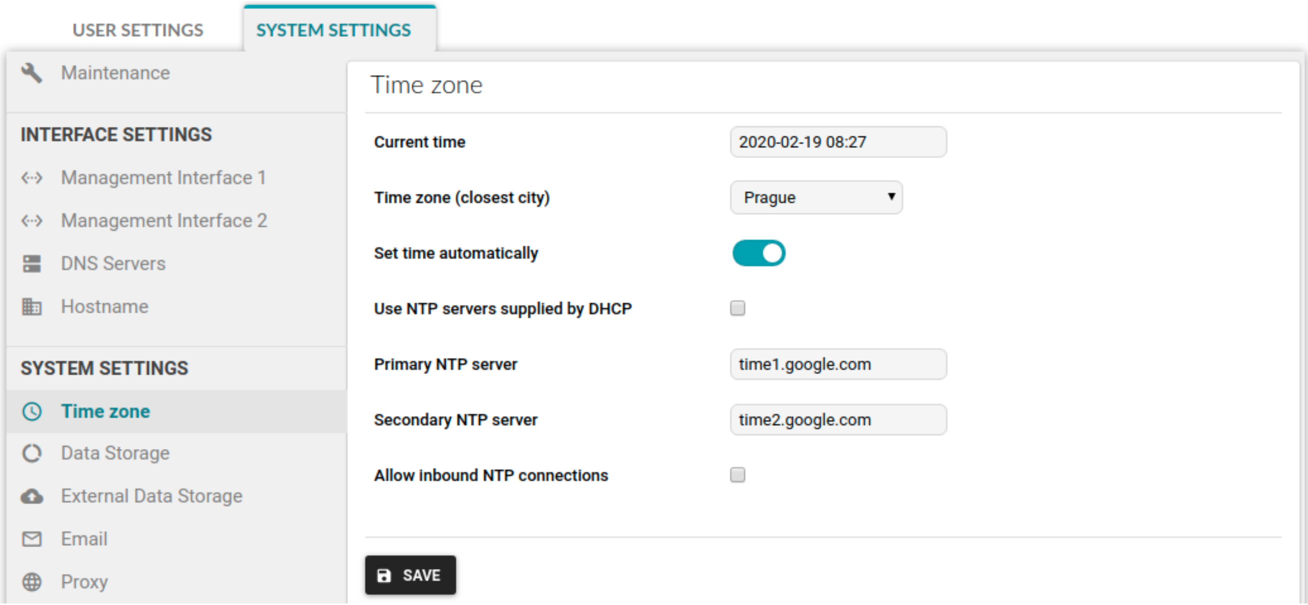
Timezone

Use this page to set the time-related configuration of your device. It is recommended to turn on automatic time synchronization with the NTP service. This function can be enabled with option **Set time automatically**. Choose the closest city and enter time servers. If you select **Use NTP servers supplied by DHCP**, then the NTP servers are obtained from DHCP service (requires a DHCP enabled for management interface as well).

You can turn on the NTP server on Flowmon device by enabling option **Use NTP servers supplied by DHCP**. The NTP server requires several minutes until its clock are stabilized. During this period, the NTP server does not respond to NTP clients' requests.

It is recommended to use time synchronization to allow the device to set the right timestamps in generated NetFlow data.

Press **Save** to apply the changes. If you perform this settings for the first time on your brand new device, it is highly recommended to clear a database after this step (see the section Built-In Collector).



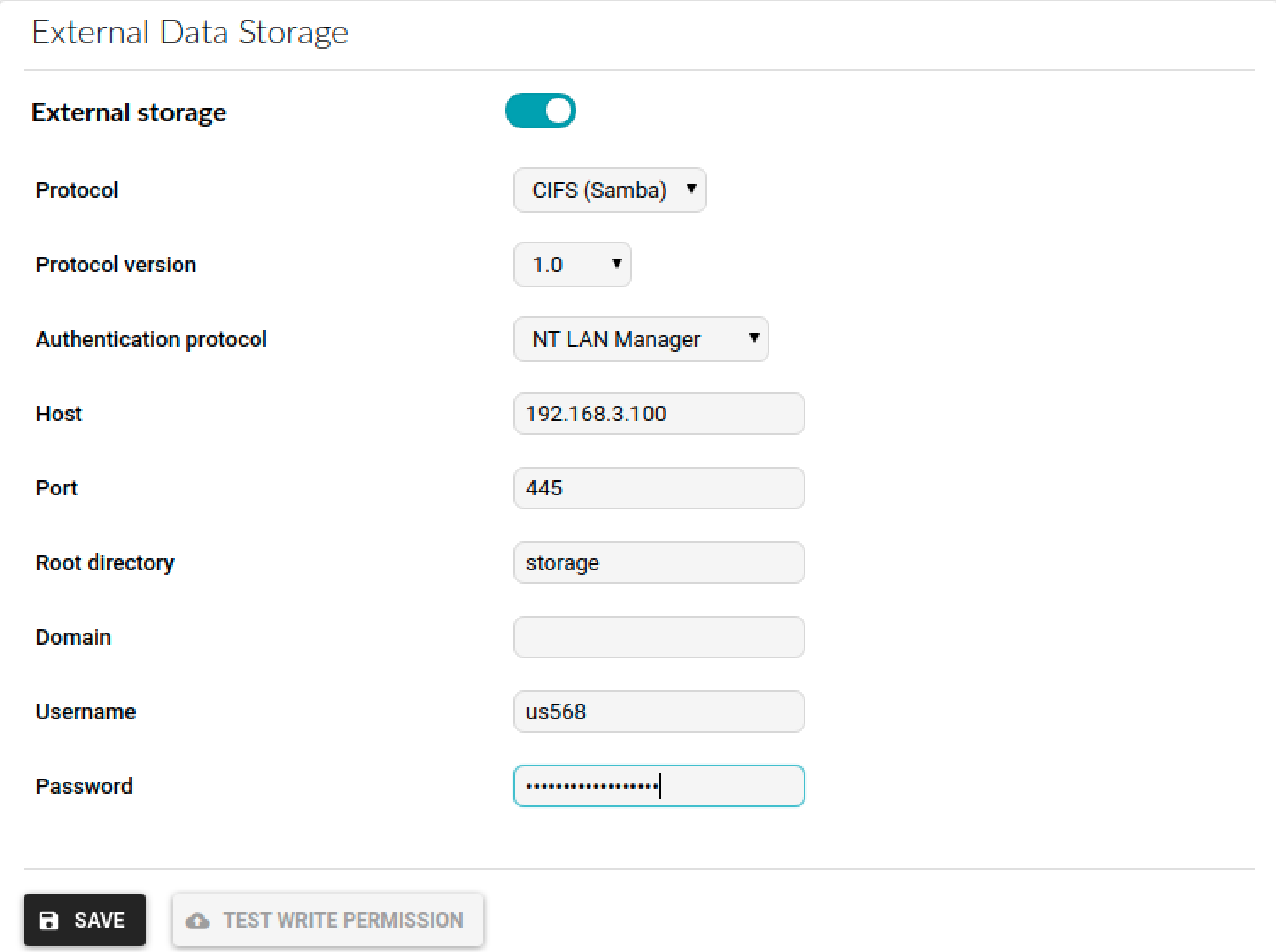
Time zone

Current time	2020-02-19 08:27
Time zone (closest city)	Prague
Set time automatically	●
Use NTP servers supplied by DHCP	□
Primary NTP server	time1.google.com
Secondary NTP server	time2.google.com
Allow inbound NTP connections	□

External Data Storage

Specific data like PDF reports or flow database backups can be stored on a remote 3rd party storage. This storage can be connected by Samba (CIFS) protocol. Select a supported protocol from the **Protocol** drop-down menu and in **Host** field enter a hostname or IP address. Enter the respective values into fields **Port**, **Root directory**, **Domain**, **Username** and **Password** and check the configuration by clicking on button **Test write permission**. This button will display a form for entering a local directory in Root directory, which will be tested for write permissions. If you leave a default value "/", then Root directory itself will be tested. If the connection and write permissions are working correctly, you will see a "Connection is OK" message.

This test can take few minutes. The **Save** button saves the configuration and checks connection to the storage (no write permissions test is performed).

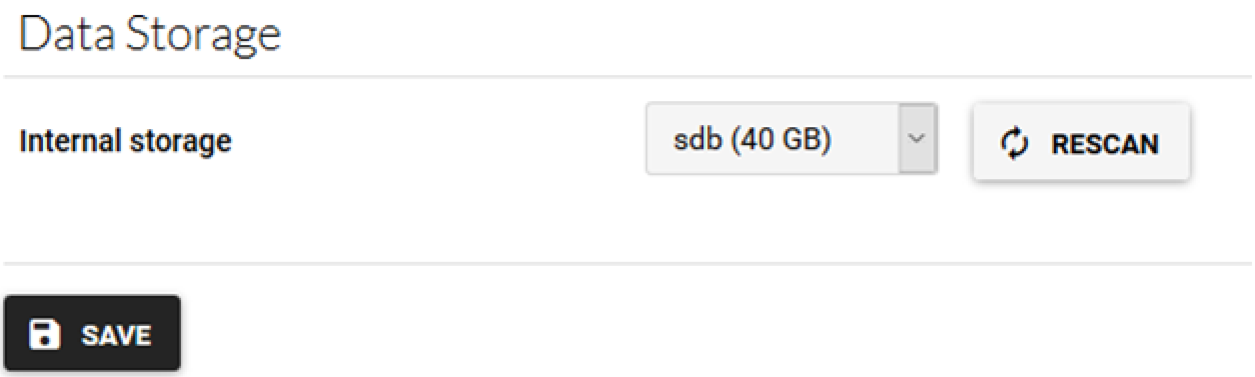


External Data Storage

External storage	●
Protocol	CIFS (Samba) ▾
Protocol version	1.0 ▾
Authentication protocol	NT LAN Manager ▾
Host	192.168.3.100
Port	445
Root directory	storage
Domain	
Username	us568
Password	•••••••••••••••••••

Data Storage (on a virtual platform)

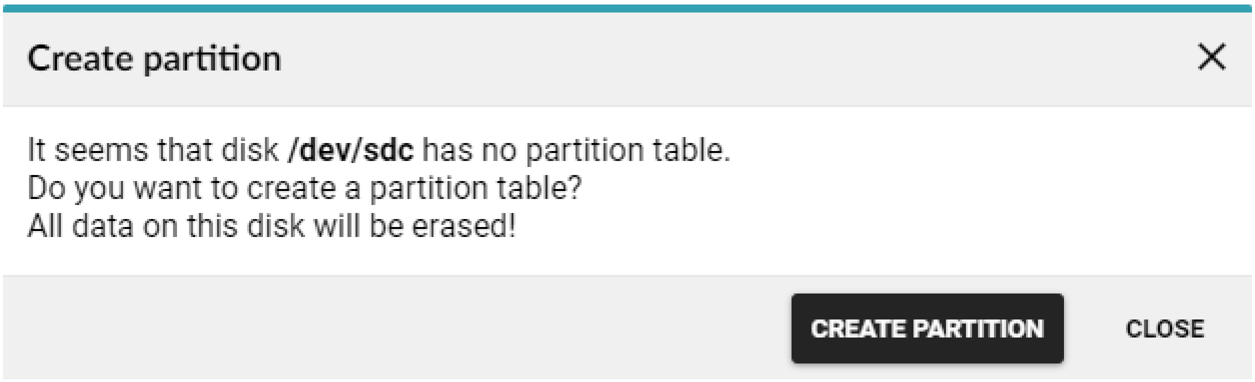
If you run the device as a virtual appliance in a virtual environment, you are able to migrate the traditional Flowmon database storage to a different disk (e.g. disk array, or other disk used by virtual machines). It could be new empty disk or shared disk array used by other applications. You can select the desired disk from drop down menu (list of available disks can be updated by clicking the **Rescan** button). Confirm the selection by pressing the **Save** button. System will check the selected disk and verify the partition table and filesystem (only EXT3, EXT4 and XFS filesystems are supported). If there are any files or directories present on the new disk, the system compares their names to those present on the old disk. The files and directories with same colliding names will be replaced! The migration operation is finished by rebooting the device. Thus the reboot can take (much) more time than usually, because all the data are being copied and checked.



Internal storage sdb (40 GB)

Data storage selection panel

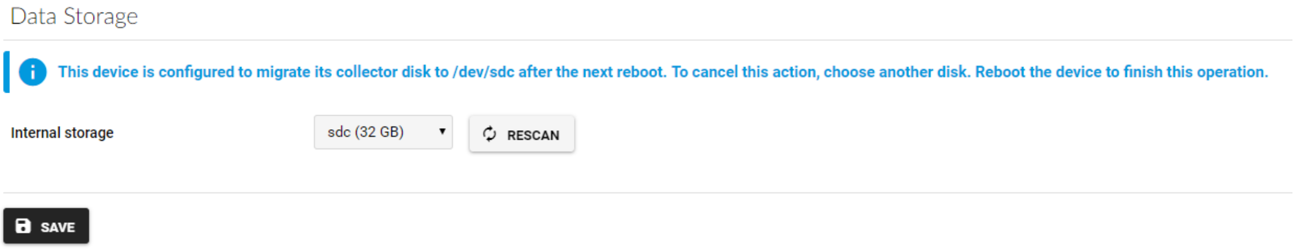
If the new disk has no partition table (for example new data storage created in virtual environment), the system will alert this and ask the user to create new partition table by clicking on the button **Create partition**. This will destroy all data on this disk!



It seems that disk **/dev/sdc** has no partition table.
Do you want to create a partition table?
All data on this disk will be erased!

The new partition table confirmation

When this operation is confirmed, the new partition table is created and system is configured to perform the data migration. Until the device is restarted, this action can be canceled anytime by choosing the original storage in the selection. If it is not canceled, then during the reboot the disk is formatted to EXT3/4 (<16TB) or XFS (>16TB) filesystem and data are copied from the original storage. If everything is done correctly, then the system will boot with the new storage. If any error occurs, system will boot with the original storage.



This device is configured to migrate its collector disk to /dev/sdc after the next reboot. To cancel this action, choose another disk. Reboot the device to finish this operation.

Internal storage sdc (32 GB)

Information about planned migration to new storage

During the disk check, the following scenarios may occur:

- New disk has no partition table (described above) - user will be asked whether to create a new partition table. If so, the system will be configured to perform new disk formatting to EXT3/4 or XFS and data migration.
- New disk has a valid partition table and is not formatted - during the device reboot the disk is formatted to the EXT3/4 or XFS filesystem and data are copied.
- New disk is formatted to a filesystem different from EXT3/4 or XFS - migration will not be performed and an error will be alerted.

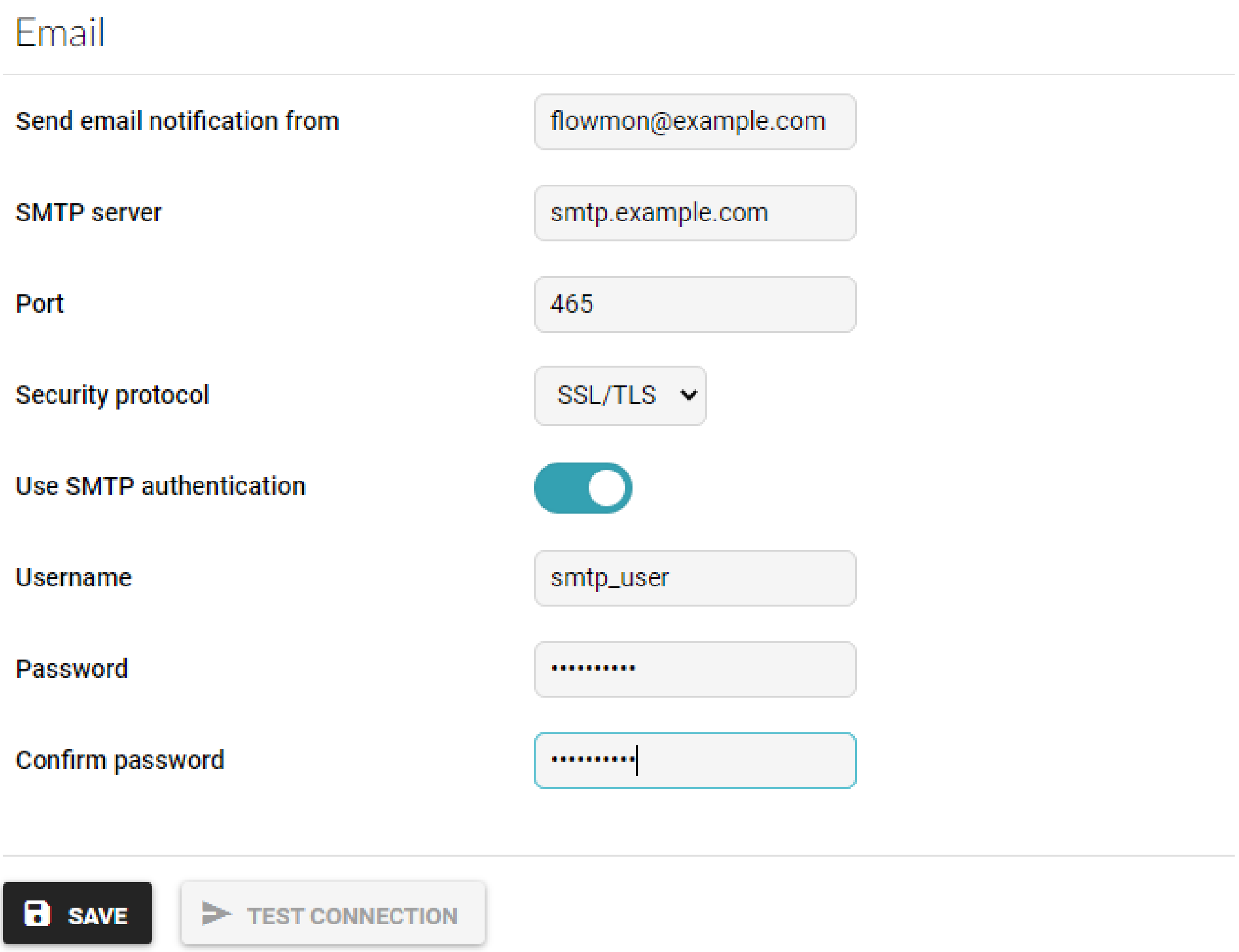
- New disk is formatted to the EXT3/4 filesystem and is smaller than 16 TB and contains files or directories with the same names as on the old disk (i.e. their names collide) - the user is warned that some files or directories on the new disk will be overwritten.
- New disk is formatted to the XFS filesystem and is bigger than 16 TB and contains files or directories with the same names as on the old disk (i.e. their names collide) - the user is warned that some files or directories on the new disk will be overwritten.
- New disk is formatted to the XFS filesystem and is smaller than 16 TB - during the device reboot the disk is formatted to the EXT3/4 filesystem and data are copied.
- New disk is formatted to the EXT3/4 or XFS filesystem and do not contain any files or directories with colliding names - during the device reboot the data will be copied from original disk to the new one.

Email

To receive email from your device, it is necessary to specify your email account and server. Please, enter the **Send email notification from** address that will be used as the default sender address and the **SMTP server** domain name or IP. Choose an encryption in the **Security protocol i**n the drop-down menu - this will fill the default value into the **Port** field. If your SMTP server uses an authorization mechanism, please, check the **Use SMTP authentication** option and set your user name and password. Your password is encrypted and a regular user cannot read it. Press **Save** to apply the changes.

⚠

Depending on their configuration, some Flowmon modules or components may use a different sender address than the one specified in **Send email notification from**. Please, make sure your SMTP server is configured to accept emails with a sender address that differs from the one configured in **Send email notification from**.



Email

Send email notification from	flowmon@example.com
SMTP server	smtp.example.com
Port	465
Security protocol	SSL/TLS
Use SMTP authentication	●
Username	smtp_user
Password	••••••••••
Confirm password	••••••••••

Proxy

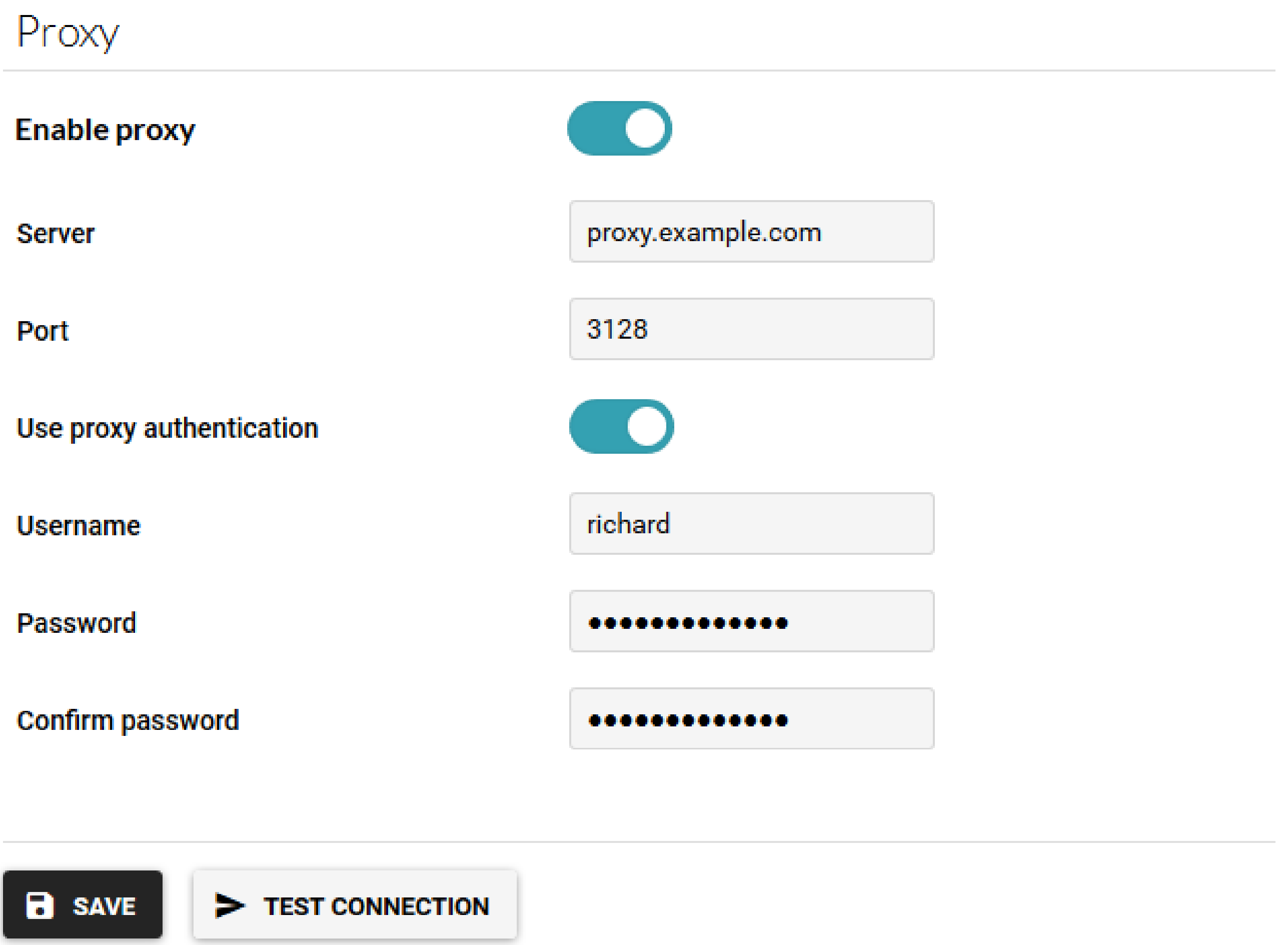
Use this page to configure a proxy server that should provides access to external resources (auto-update, blacklists, etc.). Fill-in the proxy server's address, port and, optionally, a username and password that should be used for authentication to the proxy server. You can apply the configuration by clicking the **Save** button. Configuration can be tested by clicking the **Test connection** button. This test tries to connect to services.flowmon.com using the configured proxy server.

Certificate verification is a mandatory step for all connections to external resources secured with SSL/TLS. In order to establish a secure connection via the configured proxy server, the Flowmon appliance has to be able to verify the proxy server's identity by verifying its server certificate. This process requires a trusted Certificate Authority (CA) certificate. If the connection test fails, try adding the proxy server's CA certificate in **Configuration Center - System - System Settings - Certificate Management**.

ⓘ **Certificate Authority**

A certificate of a Certificate Authority (CA) is not the server certificate issued to your proxy server. It is the certificate that issues or signs the certificate of your proxy server.

The proxy settings page



Proxy

Enable proxy: ●

Server: proxy.example.com

Port: 3128

Use proxy authentication: ●

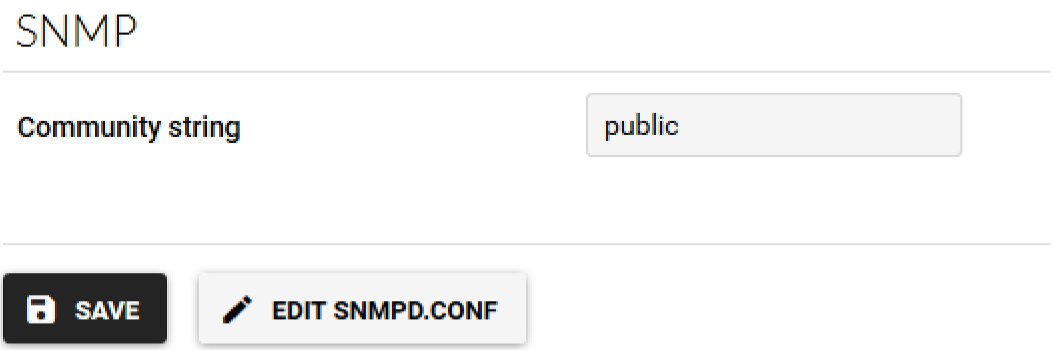
Username: richard

Password: •••••••••••••

Confirm password: •••••••••••••

SNMP

Use this page to configure the community string to access the SNMP service on the device. To allow configuration of the community string in GUI, it is required that the configuration file snmpd.conf is unmodified. If it is modified, then the community string must be configured manually in the configuration file by clicking the **Edit snpmd.conf** button. You can apply the SNMP configuration by clicking the **Save** button. This will restart SNMP service as well.



SNMP

Community string: public

The SNMP settings page

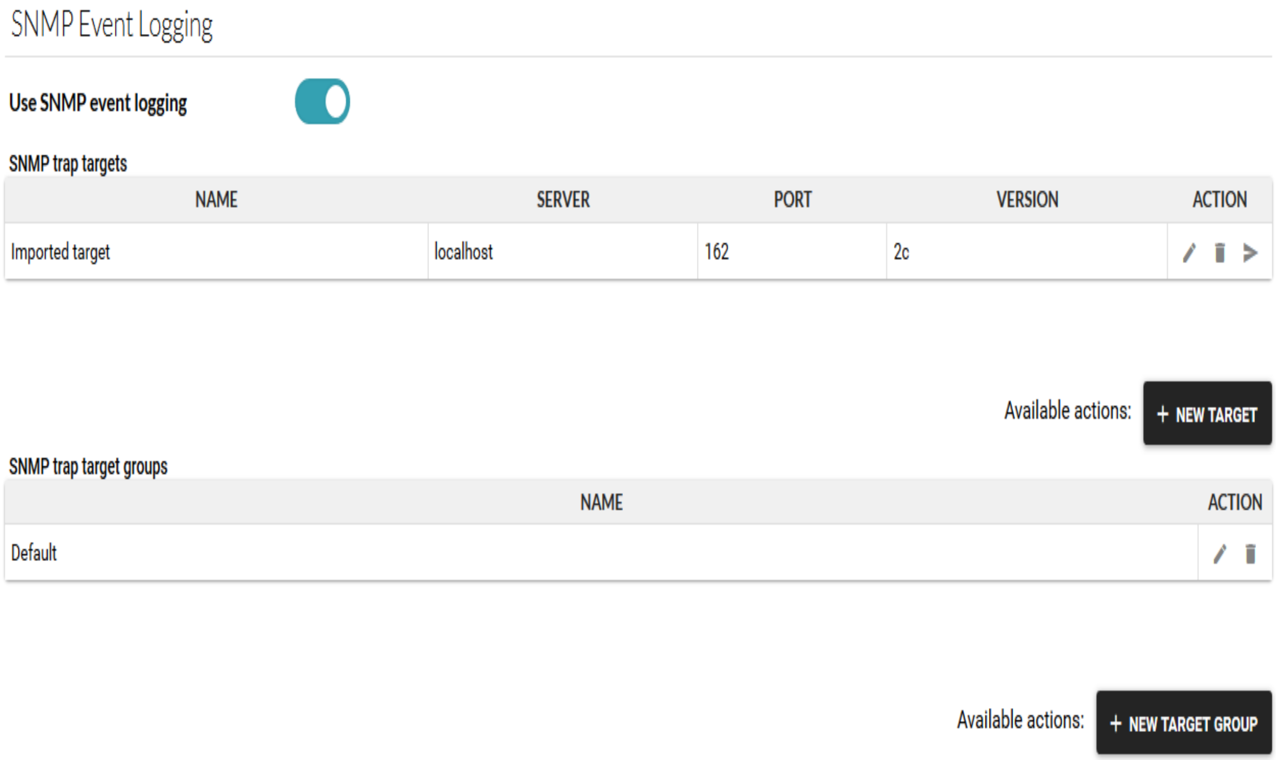
SNMP Event Logging

This page provides configuration of SNMP trap targets. To enable the SNMP traps, check the toggle switch **Use SNMP event logging**. Then, you may configure multiple SNMP trap targets and assign them into multiple target groups. New target can be created by clicking the **New Target** button. Current target can be modified by clicking the **Edit** icon in the **Action** column of the SNMP trap targets table. In the target configuration form, there can be selected a protocol version. For version 1 and 2c, **Community string** has to be defined. For version 3, community string is not available and value of **SNMPv3 parameters** must be defined instead, representing **Common options** as defined in the snmptrap manual. See the following example from the snmptrap manual:

```
snmptrap -v 3 [COMMON OPTIONS] AGENT uptime trap-oid [OID TYPE VALUE]...
```

COMMON OPTIONS must be defined in **SNMPv3 parameters**, other parameters are generated from other options and be calling application itself.

Click **Save** to apply the changes.



SNMP Event Logging

Use SNMP event logging ●

SNMP trap targets

NAME	SERVER	PORT	VERSION	ACTION
Imported target	localhost	162	2c	✎ 🗑 ▶

Available actions: + NEW TARGET

SNMP trap target groups

NAME	ACTION
Default	✎ 🗑

Available actions: + NEW TARGET GROUP

The SNMP logging settings page

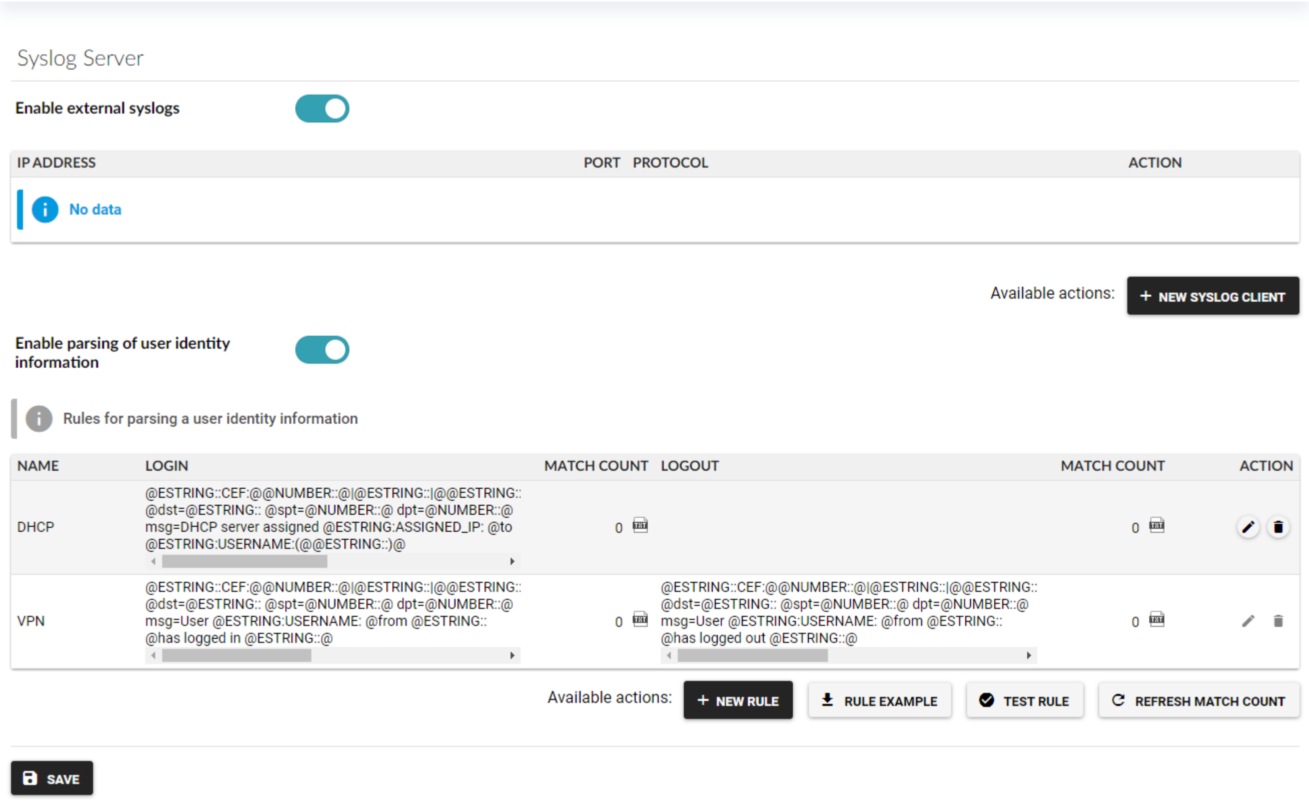
Syslog Server

This page serves for configuration of the syslog server functionality on the device. You may perform this by checking the **Enable external syslogs** toggle switch, which displays a list of allowed syslog clients. A new syslog client can be added by clicking the **New syslog client** button.

Device is able to process the syslog messages from services like DHCP, VPN or directory services and use them to collect information about user logins. This information can be used for assignment of user identity to IP address, etc. by adding a parsing rule for syslog message. The parsing rule is used by syslog-ng patterndb parser. It allows you to describe a syslog message in the similar way as regular expressions and specify which parts of the log are matching the IP address and user name.

Attention

TCP multiline syslog messages are not supported!



IP ADDRESS	PORT	PROTOCOL	ACTION
No data			

NAME	LOGIN	MATCH COUNT	LOGOUT	MATCH COUNT	ACTION
DHCP	@ESTRING::CEF:@@NUMBER::@|@ESTRING::|@@ESTRING:: @dst=@ESTRING:: @spt=@NUMBER::@ dpt=@NUMBER::@ msg=DHCP server assigned @ESTRING:ASSIGNED_IP: @to @ESTRING:USERNAME:(@@ESTRING::)@	0		0	
VPN	@ESTRING::CEF:@@NUMBER::@|@ESTRING::|@@ESTRING:: @dst=@ESTRING:: @spt=@NUMBER::@ dpt=@NUMBER::@ msg=User @ESTRING:USERNAME: @from @ESTRING:: @has logged in @ESTRING::@	0	@ESTRING::CEF:@@NUMBER::@|@ESTRING::|@@ESTRING:: @dst=@ESTRING:: @spt=@NUMBER::@ dpt=@NUMBER::@ msg=User @ESTRING:USERNAME: @from @ESTRING:: @has logged out @ESTRING::@	0	

Before you add a new parsing rule, you should check whether it will be able to get the information from the log message. You can use the **Test rule** button which shows a new form, in which you may enter the syslog message and a corresponding parsing rule. **Test result** displays the content of all variables, with the most important being **USERNAME** and **ASSIGNED_IP**. These two variables must be filled with corresponding data for user identity to work. An optional variable **DOMAIN** can be used to specify the domain name, which is then added to the USERNAME in the following format: DOMAIN\USERNAME. If the DOMAIN is not specified, USERNAME stays in the original format. To create parsing rules by yourself, you need to follow the syntax of syslog-ng patterndb, which is available in the syslog-ng documentation.

Note

In Logout message rule, the **ASSIGNED_IP** is not mandatory - only **USERNAME** must be present. If **ASSIGNED_IP** is missing, system will use IP address assigned to this **USERNAME** in login message. If the **USERNAME** was assigned to multiple concurrent IP addresses, then the logout message requires also **ASSIGNED_IP** information for proper procession of logout message.

Parsing Rules Syntax

It is usually enough to use the **ESTRING** data type, which matches any string ended by specified string or character. **@ESTRING::ip address=@** matches any text ended by a string 'ip address='.

@ESTRING::ip address=@@ESTRING:ASSIGNED_IP:@ matches for example this string: 'DHCP ip address=192.168.1.1' and fills the variable ASSIGNED_IP by value '192.168.1.1'.

@ESTRING::ip address=@@ESTRING:ASSIGNED_IP: user=@@ESTRING:USERNAME:@ matches for example this string: 'DHCP ip address=192.168.1.1 user=flowmon' and fills the variable USERNAME with value ’flowmon’.

In case you need to create a parsing rule for a log message, in which the words are separated only by white spaces, for example: ’DHCP 192.168.1.1 MSWinEventLog flowmon’, then you can use following parsing rule:

@ESTRING::DHCP @@@ESTRING:ASSIGNED_IP:MSWinEventLog@@ESTRING:USERNAME:@, where

@ESTRING::DHCP @ matches the string until the first space after the word ’DHCP’.
@ESTRING:ASSIGNED_IP:MSWinEventLog@ matches the string from the first space after the word ’DHCP’ until the word ’MSWinEventLog’.

@ESTRING:USERNAME:@ matches the string from the word ’MSWinEventLog’ until the end of the string.

If you try this example using the tool **Test rule**, then in the **Test result** section you will see that the variables USERNAME and ASSIGNED_IP are surrounded by additional white spaces. These will be removed internally later, so you don’t have to try removing them by a parsing rule.

After you insert a new parsing rule, there is another option how to validate that it’s correct. In the table **Rules for parsing User Identity information** there is a column **Match count**, which shows how many log messages matched this rule. Specific log messages can be displayed by clicking on the picture of a file in the same column.

All parsing rules must contain some combination of strings which is specific only for this log. For example, if you want to parse information from Windows Active Directory, the simple version of the log message could look like this:

’<38>Jun 1 15:30:28 microsoft-windows-security-auditing[success] 4624 An account was successfully logged on.Account Name:FlowmonAccount Domain:INVEAName:Source Network Address:192.168.1.1Source Port:50625’.

There could be multiple versions of this message for logout or error messages, so you need to specify the parsing rule to match only this type of message. You can start from a static part of the log, which specifies what kind of service this: ’microsoft-windows-security-auditing[success]’. Then you need to know if this is really login message, so match the string: ’An account was successfully logged on’. And finally extract information about IP address and user name. Resulting parsing rule looks like this:

@ESTRING::microsoft-windows-security-auditing[success]@@ESTRING::An account was successfully logged on.@@ESTRING::Account Name:@@ESTRING:USERNAME:Account Domain:@@ESTRING::Source Network Address:@@ESTRING:ASSIGNED_IP:Source Port:@

ⓘ **Note**

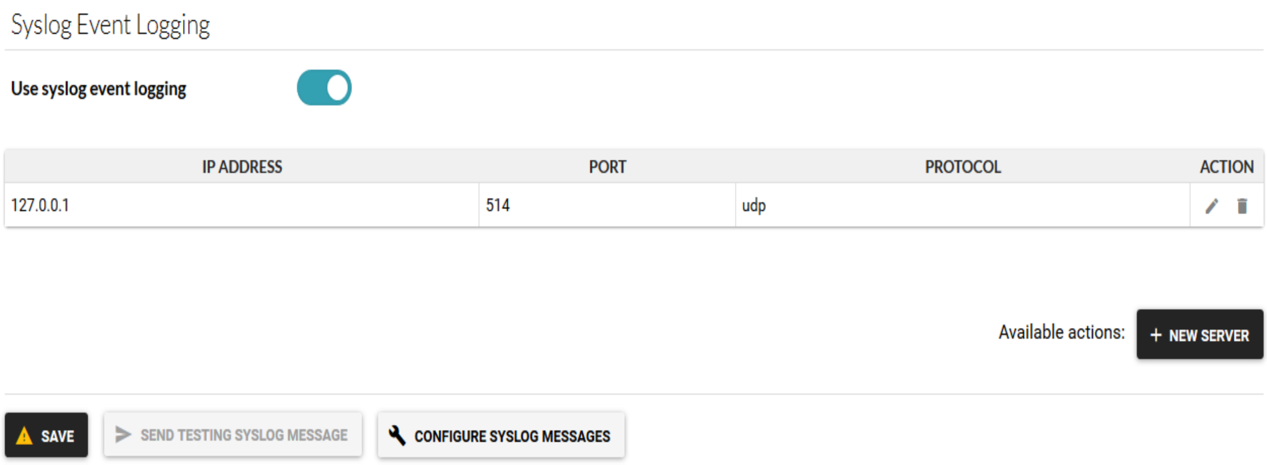
The parser ignores the newline characters (CR, LF) in multi-line messages. Do not use them in your parsing rules.

To obtain more information about how to write parsing rules, see the official syslog-ng documentation:

Syslog Event Logging

Configuration of syslog message sending is located in this panel. To allow message sending, check the toggle switch, add a new server and press **Save** to apply the changes. To check the entered data, press

Send testing syslog message button.



Syslog Event Logging

Use syslog event logging ●

IP ADDRESS	PORT	PROTOCOL	ACTION
127.0.0.1	514	udp	✎ 🗑

Syslog logging settings page

LDAP

LDAP and tenants

In the current version, users from LDAP and TACACS+ are created in the base tenant only.

Note

For proper functionality the LDAP server has to support LDAP MemberOf function.

In case you’re using OpenLDAP as your LDAP server please make sure, that your group entries contain attribute "objectClass" with value set either to "groupofuniquenames" or to "groupofnames" and that every account entry contains attribute "objectClass" with value set to "person".

User authentication can be done either according to local database or according to directory services, e.g. LDAP server.

Information about LDAP settings:

- **Server:** enter IP address or domain name of LDAP server
- **Port:** enter port, default is 389 and 636 for encrypted connection (SSL)
- **User bind DN:** full path to user, who is to be used for LDAP connection.

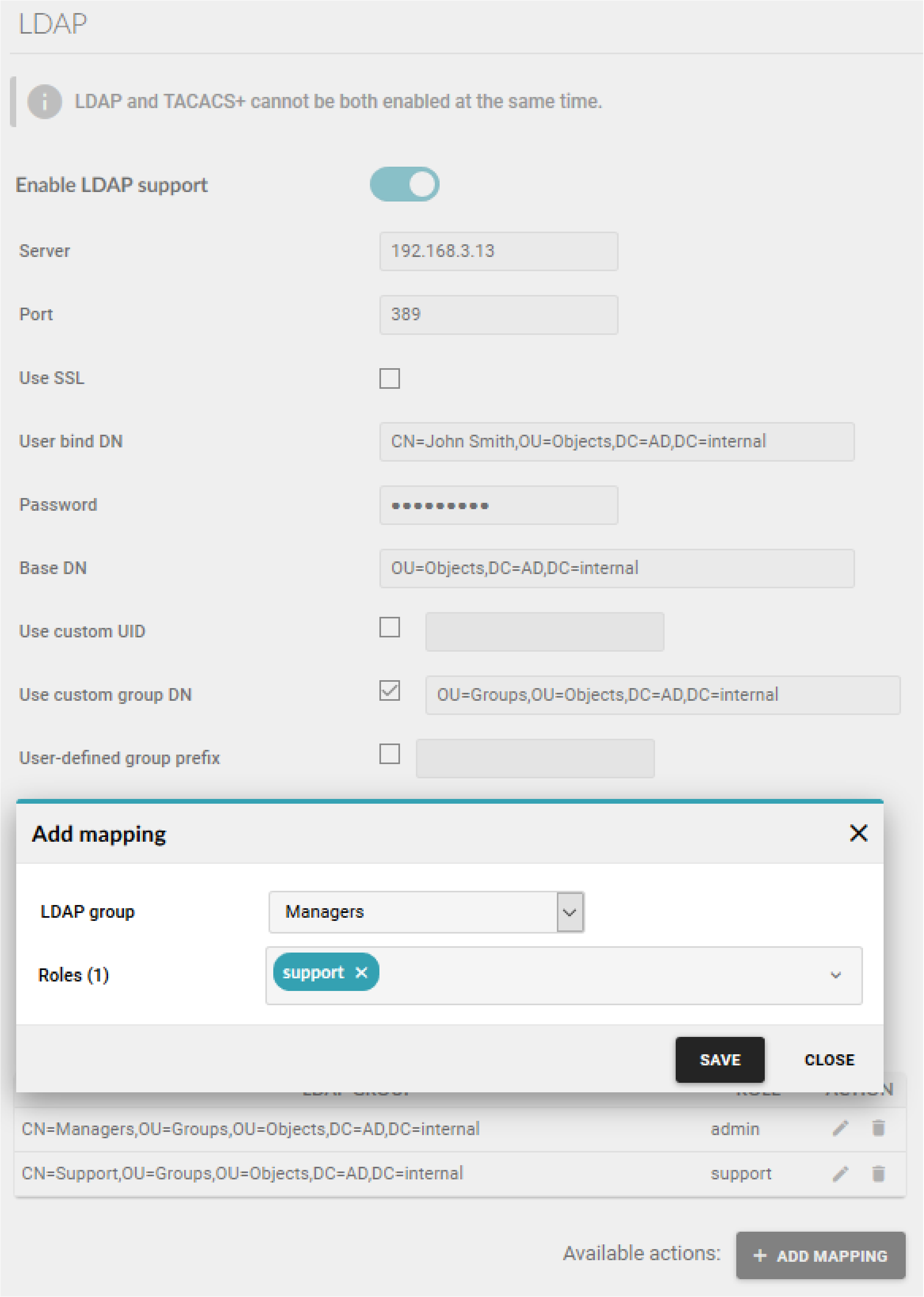
  Note

  Attention, in Active Directory you need to use both first name and surname (**cn** value). The Flowmon login is stored in **sAMAccountName** value

LDAP service	User bind DN
Active Directory / LDAP	CN=Administrator Name,CN=Users,DC=invea,DC=cz
Directory Server / OpenLDAP	uid=administrator,ou=People,dc=invea,dc=cz

Table 2: LDAP configuration examples

- **Password:** for account in **User bind DN**
- **Base DN:** default search point. Only users in this node and its subnodes will have access to Flowmon. Base DN value is mostly all DC parameters (eg. **DC=invea,DC=cz**)
- **Use custom UID:** set LDAP attribute to compare with Flowmon login. Default value is uid (for openLDAP) or sAMAccountName (for Active Directory)
- **Use custom group DN:** you can set different default search point for groups. If selected, only groups in this node and its subnodes will be used by Flowmon
- **User defined group prefix:** set your group prefix in LDAP (please see below)
- **Group delimiter:** set the delimiter character between group prefix and role name
- **Use group nesting:** In an LDAP directory, a nested group is defined as a child group entry whose DN (Distinguished Name) is referenced by an attribute contained within a parent group entry. Flowmon allows to use this nesting for inheritance of access rights
- **Group nesting type:**
    - **Inherit from parent:** Groups inherit access rights from their parent groups
    - **Obtain from child:** Groups inherit access rights from their child groups
- **Enable mapping:** If enabled, it is possible to map existing LDAP groups to one or more Flowmon roles. All users that are members of the mapped group get the access rights from the mapped roles



LDAP

LDAP and TACACS+ cannot be both enabled at the same time.

Enable LDAP support	●
Server	192.168.3.13
Port	389
Use SSL	□
User bind DN	CN=John Smith,OU=Objects,DC=AD,DC=internal
Password	••••••••••
Base DN	OU=Objects,DC=AD,DC=internal
Use custom UID	□
Use custom group DN	☑ OU=Groups,OU=Objects,DC=AD,DC=internal
User-defined group prefix	□

Add mapping

LDAP group	Managers
Roles (1)	support ✕

CN=Managers,OU=Groups,OU=Objects,DC=AD,DC=internal	admin	✎ 🗑
CN=Support,OU=Groups,OU=Objects,DC=AD,DC=internal	support	✎ 🗑

Available actions:

LDAP Settings page

Connection Errors

- **LDAP Connect:** bad server, port or use of SSL encryption
- **LDAP Bind:** bad User bind DN or user password
- **LDAP Search:** bad Base DN, cannot load any group from LDAP

If you are able to connect to LDAP server, save your settings by clicking on **Save** button.

If LDAP support is enabled, system works as follows

1. **During user log in, Flowmon server tries to connect to LDAP server**
    - **Success** - user authentication was successfull. In case of first log in, user account is created in local database according to LDAP account. Then during every login, the local account data are compared with LDAP account data. If a difference is found, it will retrieve the current data from LDAP. Any changes in the local user account are reported by information message.
    - **Failure** - connection failed. Error message is displayed. In this case, user **admin**, who is not using LDAP authentication, can log to system. Other users saved in local database, who are not in LDAP, can log in too.

2. **Credentials check is performed**
    - **Success** - user authentication was successful. In case of first log in, user account is created in local database according to LDAP account. Then during every login, the local account data are compared with LDAP account data. If a difference is found, it will retrieve the current data from LDAP. Any changes in the local user account are reported by information message.
    - **Failure** - authentication failed. User is asked to enter new credentials

User admin is managed in special way. For this account, data are always taken from the local database and the LDAP account is never used.

User roles and access-rights settings for LDAP user

LDAP user is automatically assigned with roles according to their groups in LDAP. To assign a role to user, the group name must be in the format <prefix><group delimiter><role name>, where **prefix** is one of the following: **flowmon**, **inveaos** or **User defined group prefix**. For more information about Role name, please see the User Settings chapter.

group delimiter is either dash, or underscore character

Users assigned to group **<prefix><group delimiter>admin** has granted administrator rights and can access every module.

Role mapping and nesting examples

1. Inherit from parent option

There are LDAP groups A and A1 and A2, LDAP groups A1 and A2 are children of group A.
There is an existing role in Flowmon called A.
Role A has defined permissions and access to Flow Source 1.
Group A is mapped to role A.
Groups A1 and A2 are children of Group A, therefore they inherit both access rights of role A and also have access to Flow source 1.

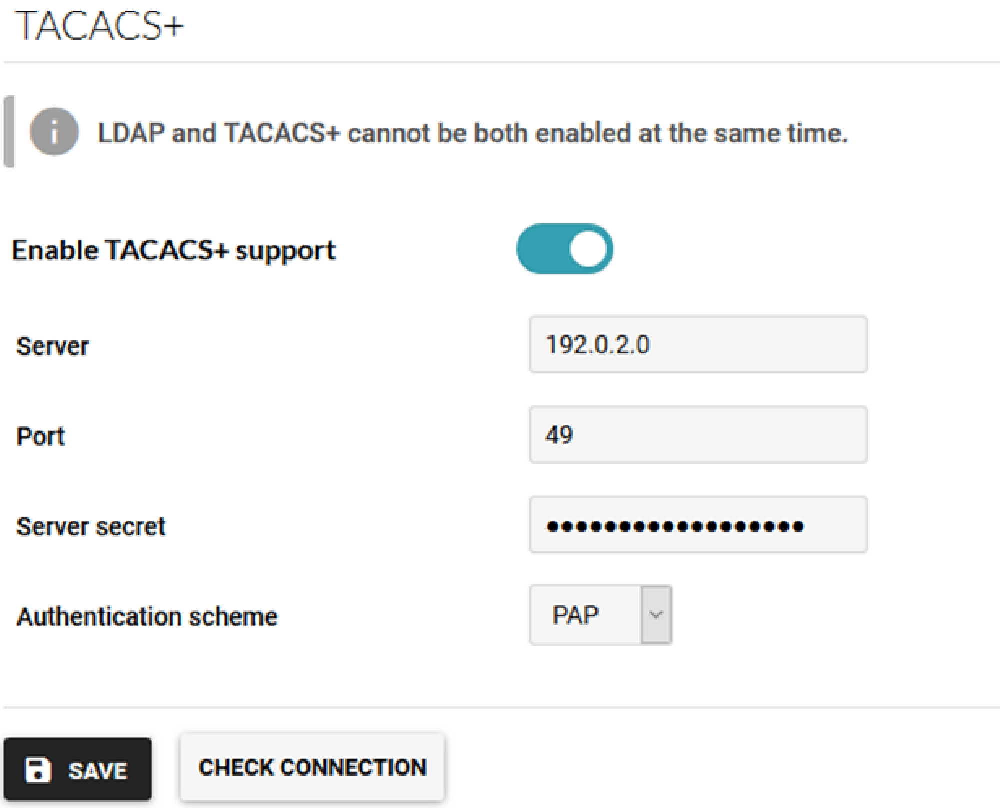
2. Obtain from child option

There are LDAP groups A and A1 and A2, LDAP groups A1 and A2 are children of group A.
There are existing roles in Flowmon called A and B.
Role A has defined permissions and access to Flow Source 1.
Role B has defined permissions and access to Flow Source 2.
Group A1 is mapped to role A.
Group A2 is mapped to role B.
Group A is the parent of groups A1 and A2, therefore it inherits both access rights of roles A and B and access to Flow Source 1 and Flow Source 2.

TACACS+

TACACS+ and tenants

In the current version, users from LDAP and TACACS+ are created in the base tenant only.



TACACS+

LDAP and TACACS+ cannot be both enabled at the same time.

Enable TACACS+ support: ●

Server: 192.0.2.0

Port: 49

Server secret: ••••••••••••••••••

Authentication scheme: PAP

User authentication can be done either according to local database or according to directory services, e.g. TACACS+ server.

Information about TACACS+ settings:

- **Server** - IP address of TACACS+ server
- **Port** - connection port (usually 49)
- **Server secret** - the secret passphrase for connection
- **Authentication scheme** - only PAP is supported

Provided connection information can be verified by clicking on button **Check connection**. You will be prompted to provide login and password information for a user recorded in the TACACS+ server directory. The system will then verify your connection.

If you are able to connect to TACACS+ server, save your settings by clicking on the **Save** button.

When TACACS+ authentication is enabled, every user will have to use their credentials from TACACS+ directory to login to the system. In opposite to LDAP, it is not possible to assign a role to a Flowmon user in TACACS+ directory. For this reason, every Flowmon user must be configured in the Configuration Center as well, where he/she will be assigned with roles. Only user configured in both TACACS+ and Configuration Center will be allowed to log into the system.

User admin is managed in special way. For this account, data are always taken from the local database and the TACACS+ account is never used.

Security Settings

Security settings include the following sections:

- IPsec Service
- Web Interface
- GPG Settings
- Certificate Management

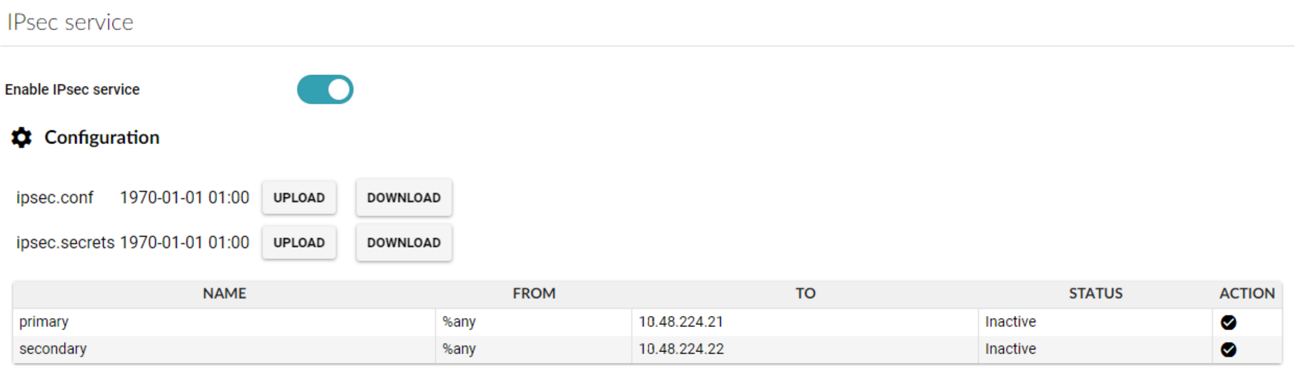
IPsec Service

This page is used for configuration of IPsec tunnels. Prior IPsec tunnel configuration, it must be enabled by **Enable IPsec service** toggle switch. Configured tunnels can be activated and deactivated in the column **Action**.

Configuration

Configuration of IPsec tunnels must be provided in the form of ipsec.conf and ipsec.secrets files.

Please, see the following links (ipsec.conf and ipsec.secrets) for more information about configuration of these files.



IPsec service

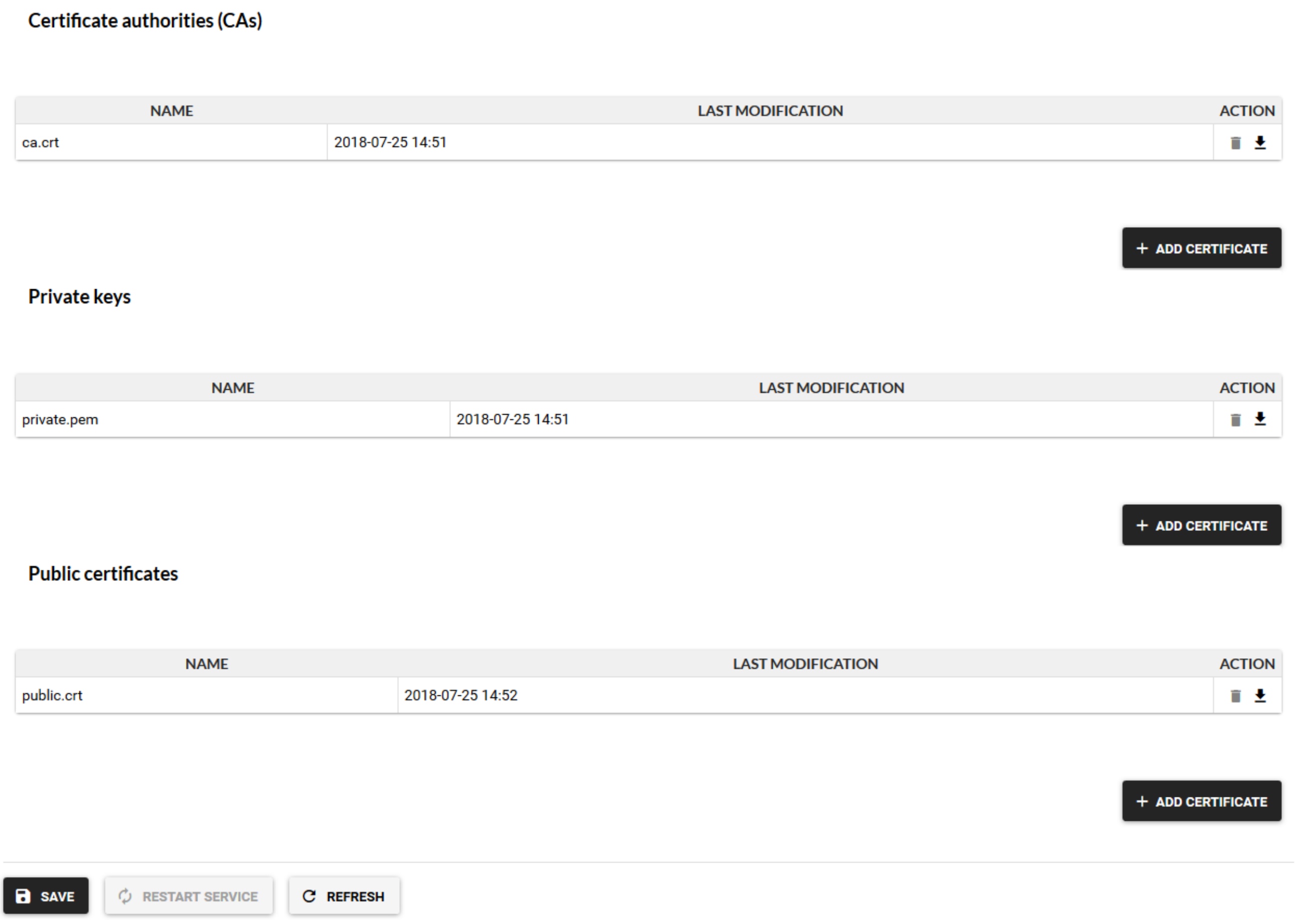
Enable IPsec service ●

Configuration

ipsec.conf 1970-01-01 01:00

ipsec.secrets 1970-01-01 01:00

NAME	FROM	TO	STATUS	ACTION
primary	%any	10.48.224.21	Inactive	✔
secondary	%any	10.48.224.22	Inactive	✔



Certificate authorities (CAs)

NAME	LAST MODIFICATION	ACTION
ca.crt	2018-07-25 14:51	

Private keys

NAME	LAST MODIFICATION	ACTION
private.pem	2018-07-25 14:51	

Public certificates

NAME	LAST MODIFICATION	ACTION
public.crt	2018-07-25 14:52	

The IPsec service certificates

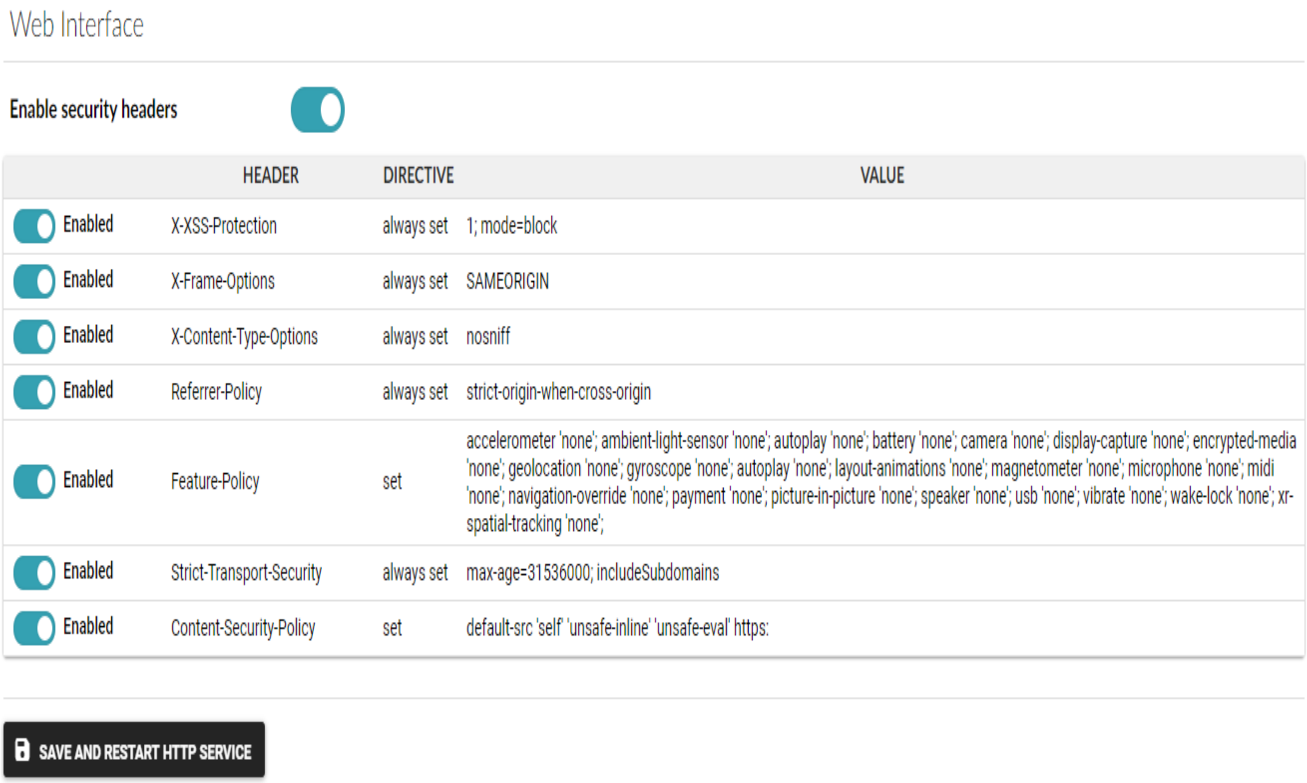
Certificates and Keys - CAs, Private keys and Public certificates

Here, the certificates for access are managed. In the first table, the CA certificate can be provided. In the second table, private key of your device can be provided for authentication to remote side. In the third table, public keys of remote sides can be provided.

Web Interface

Use this page to enable optional security features for the web interface. The following options are considered to be advanced and should be enabled only by experienced administrators who understand the implications of enabling them. Enabling options on this page may limit the usability of some features of the web interface. Potential limitations are mentioned in the description of individual features.

To enable HTTP security headers, toggle the **Enable security headers** switch.



Web Interface

Enable security headers ●

	HEADER	DIRECTIVE	VALUE
● Enabled	X-XSS-Protection	always set	1; mode=block
● Enabled	X-Frame-Options	always set	SAMEORIGIN
● Enabled	X-Content-Type-Options	always set	nosniff
● Enabled	Referrer-Policy	always set	strict-origin-when-cross-origin
● Enabled	Feature-Policy	set	accelerometer 'none'; ambient-light-sensor 'none'; autoplay 'none'; battery 'none'; camera 'none'; display-capture 'none'; encrypted-media 'none'; geolocation 'none'; gyroscope 'none'; autoplay 'none'; layout-animations 'none'; magnetometer 'none'; microphone 'none'; midi 'none'; navigation-override 'none'; payment 'none'; picture-in-picture 'none'; speaker 'none'; usb 'none'; vibrate 'none'; wake-lock 'none'; xr-spatial-tracking 'none';
● Enabled	Strict-Transport-Security	always set	max-age=31536000; includeSubdomains
● Enabled	Content-Security-Policy	set	default-src 'self' 'unsafe-inline' 'unsafe-eval' https:

Individual security headers can be enabled or disabled by toggling the corresponding switch. **Directive** and **Value** options for individual headers are immutable.

Attention

Enabling security headers may prevent you from embedding parts of the web interface in external applications. It may also interfere with third-party integrations submitting direct requests to URLs of the web interface.

To apply changes, click the **Save and Restart HTTP Service** button.

GPG Settings

On the Flowmon device a private GPG key can be uploaded, which will be used for signing out- going emails (if enabled). On page **GPG Settings**, device's private PGP key can be provided. **This key must have empty password!**

Note

Sender email address of a signed email will always be changed to the email address assigned to the signing certificate.

Each user can upload their public key for encrypting the emails sent to him (if enabled). The public key is provided in **GPG encryption certificates** panel.

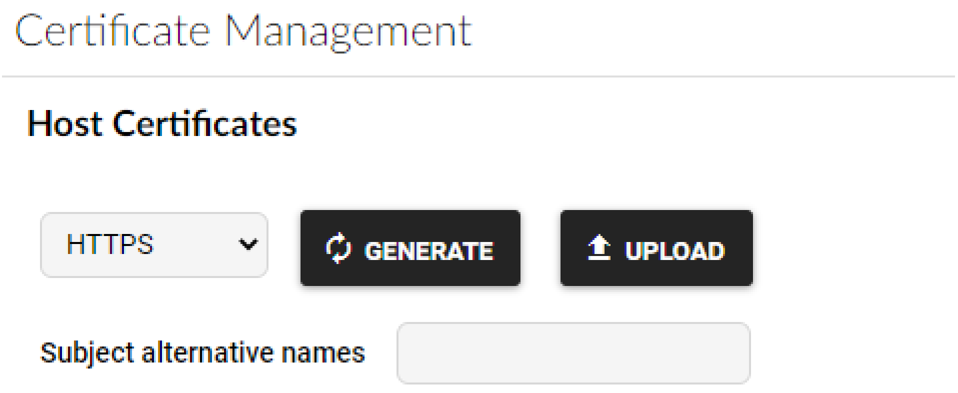
ⓘ **Note**

It is necessary to provide a public key of each user whose email is used as a recipient of encrypted email. If such key is not found, the email will not be sent and an error message will be provided.

Certificate Management

Host Certificates

When you change the hostname of your device or after the first login to the device, it is highly recommended to generate a new SSL certificate. You can generate certificates for secured HTTPS protocol or PostgreSQL database for remote connection. Before starting, select the desired value in drop-down menu. To generate the certificate, press the **Generate** button. You will be asked to confirm your choice - press the button **Save**. This will generate a new certificate, automatically signed by Flowmon Networks valid for the new hostname of your device. Finally, allow the new certificate in your browser.


Certificate Management

Host Certificates

Subject alternative names

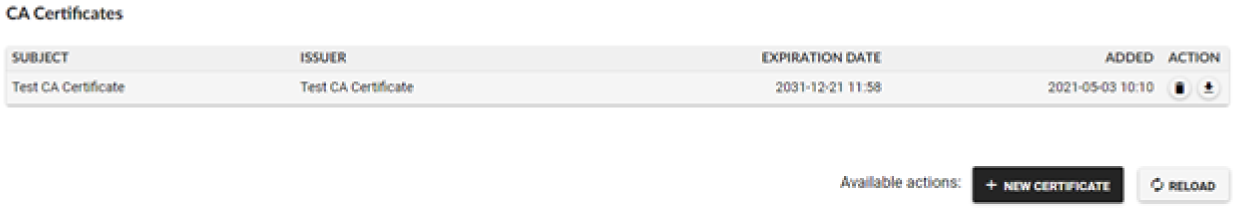
Host Certificates

If you have your own certificate generated, you can apply it by clicking the **Upload** button. Choose the certificate file (*.crt) and private key file (*.key) and click **OK**.

ⓘ Private keys protected by passphrase are not supported.

CA Certificates

In **CA Certificates**, a user can add a Certificate Authority (CA) certificate to the system. The CA certificate is used when Proxy is enabled in **Configuration Center – System – System Settings – Proxy**. When using a proxy server, the Flowmon appliance verifies the proxy server's certificate with CA certificates stored in the system. Certificate verification is needed in order to establish a secure connection with external servers. If verification fails, access to external resources, such as software updates, is denied. Verification can fail when the configured proxy server uses its own CA to generate server certificates based on user requests (SSL Bump) and the CA is not added to the system.

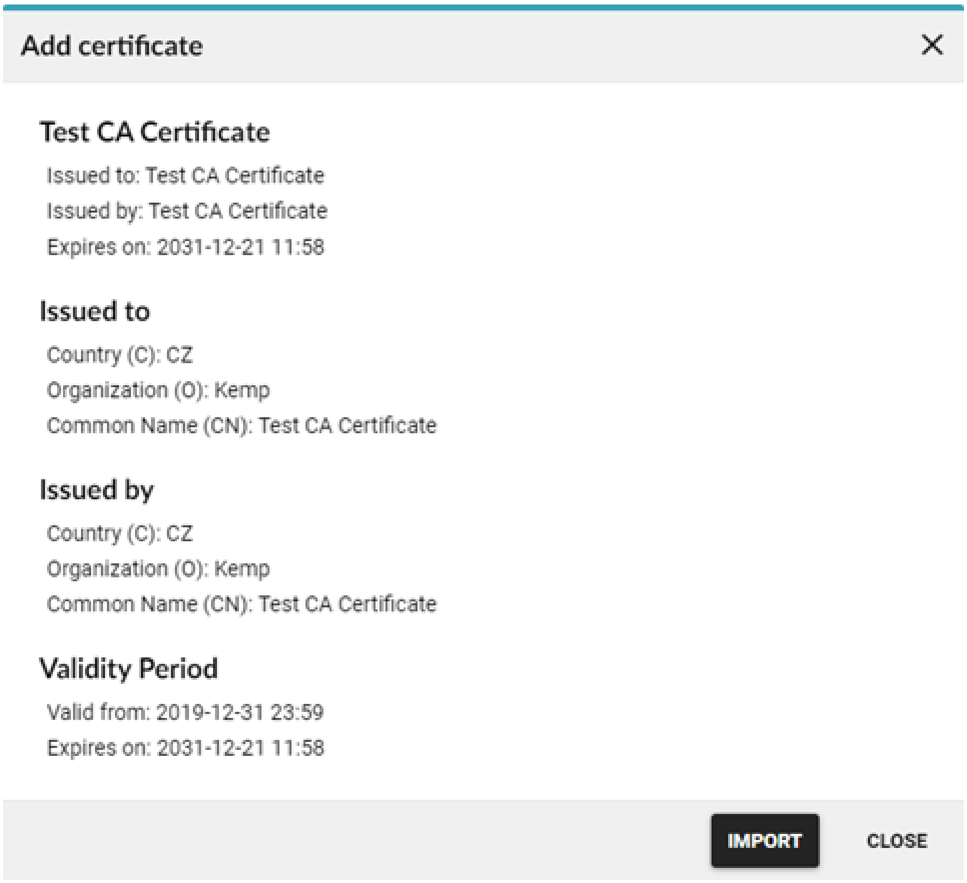


CA Certificates

SUBJECT	ISSUER	EXPIRATION DATE	ADDED	ACTION
Test CA Certificate	Test CA Certificate	2031-12-21 11:58	2021-05-03 10:10	

CA Certificates section

To add a CA certificate to the system, press the **New Certificate** button. Choose the certificate file. Only files with extensions .pem, .crt or .der are supported. The CA certificate can be either in text or binary format. Press the **Upload** button to upload the CA certificate for validation. If the CA certificate is valid, its details are displayed. To add the uploaded CA certificate, press the **Import** button. Please note that if the uploaded file contains multiple certificates, only the first one will be processed. If a trusted chain with multiple CA certificates should be added, CA certificates must be added one by one.



Add certificate

Test CA Certificate

Issued to: Test CA Certificate
Issued by: Test CA Certificate
Expires on: 2031-12-21 11:58

Issued to

Country (C): CZ
Organization (O): Kemp
Common Name (CN): Test CA Certificate

Issued by

Country (C): CZ
Organization (O): Kemp
Common Name (CN): Test CA Certificate

Validity Period

Valid from: 2019-12-31 23:59
Expires on: 2031-12-21 11:58

The Add certificate form

When adding a new CA certificate, the following requirements must be met:

- **Valid from (not before)** date is set in the past
- **Expires on (not after)** date is set in the future
- **Basic Constraints extension** contains the CA bit

When a CA certificate with an empty subject or issuer is added, its Common Name in the GUI is displayed as *Empty Common Name*.

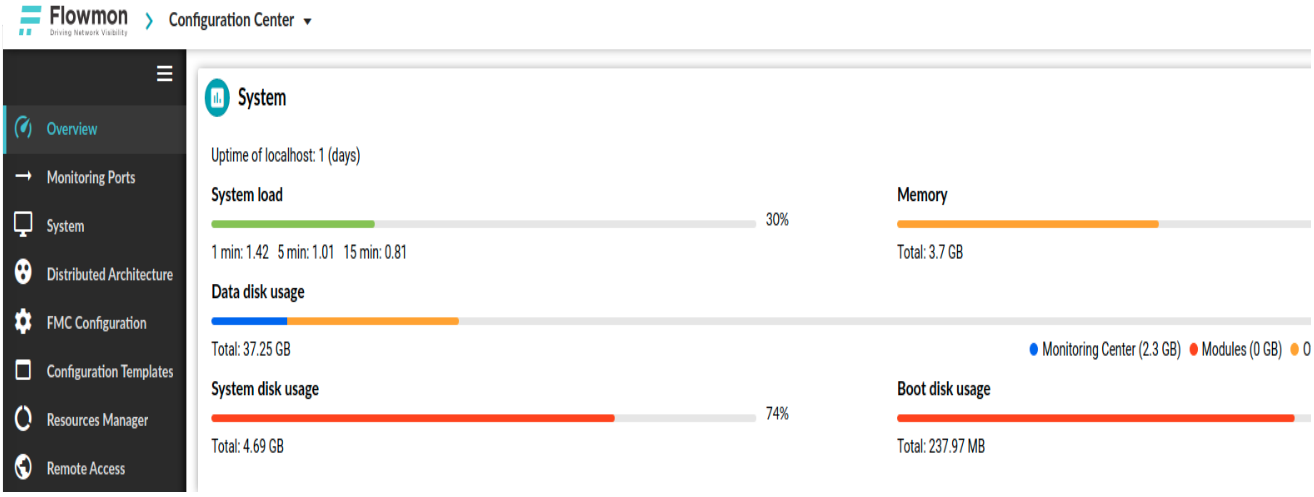
When an existing CA certificate expires, a new message will appear in System messages (the bell icon). The expiration check is done automatically every 24 hours.

Press the **Reload** button to reload all certificates added to the system. This will also check for CA certificate expiration as described above.

Each CA certificate can be deleted by pressing the **Delete** button or downloaded by pressing the **Export** button next to the CA certificate.

Overview

This page provides the Flowmon Networks device system information. Management interface status and system configuration is shown. The current status of running flow monitoring ports is displayed.



System

Uptime of localhost: 1 (days)

System load 30%

1 min: 1.42 5 min: 1.01 15 min: 0.81

Memory

Total: 3.7 GB

Data disk usage

Total: 37.25 GB ● Monitoring Center (2.3 GB) ● Modules (0 GB) ● 0

System disk usage 74%

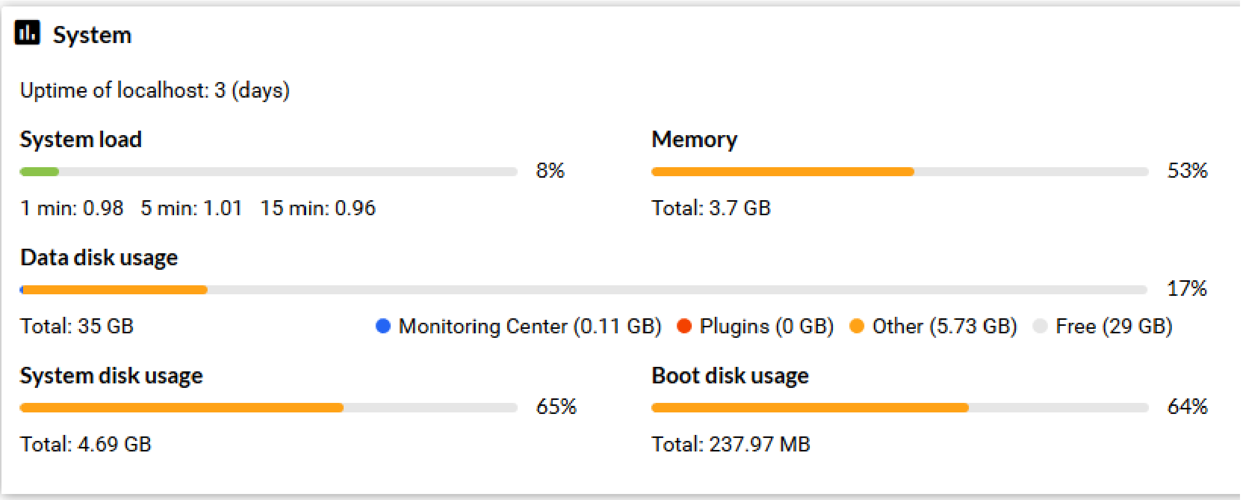
Total: 4.69 GB

Boot disk usage

Total: 237.97 MB

System

The System panel shows the current system status. The first line shows the appliance hostname, system uptime shows how long the system has been running. System load line shows the system load in last 1, 5 and 15 minutes. Memory line shows the amount of free and used memory. Last lines show space usage of Data disk, System disk and Boot disk and provide information about disc conditions obtained by SMART service (not available on virtual devices). If an error is reported by SMART, the email is sent regularly to all users with administrator privileges.



System

Uptime of localhost: 3 (days)

System load 8%

1 min: 0.98 5 min: 1.01 15 min: 0.96

Memory 53%

Total: 3.7 GB

Data disk usage 17%

Total: 35 GB ● Monitoring Center (0.11 GB) ● Plugins (0 GB) ● Other (5.73 GB) ● Free (29 GB)

System disk usage 65%

Total: 4.69 GB

Boot disk usage 64%

Total: 237.97 MB

System information panel

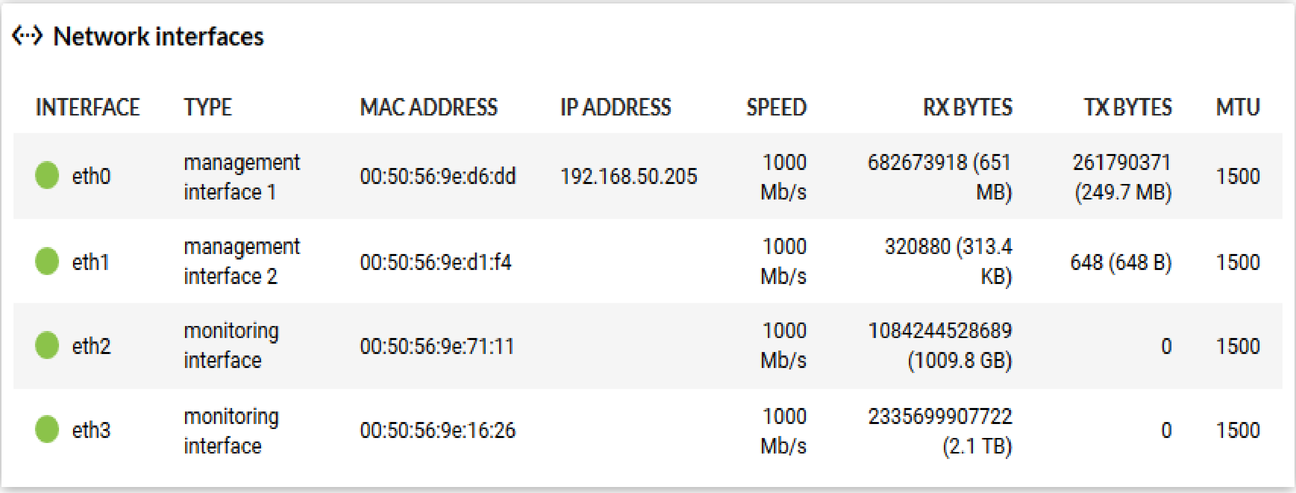
RAID status

This panel shows information about status of the RAID field (if the device includes this field). The first row shows the field type and the second the current status. When the user hovers the cursor over the state icon, a window with a list of disks present in the field and their status shows up. The icon changes its color depending on the field status - green means the optimal state, orange a degenerated state and red a critical field failure. The user will also be informed about any changes of status of the field in the system messages.

Network Interfaces

This panel shows the status of device's network interfaces. The interface led indicates link status

– red means link is down and green means link is up. The following information is available: interface type, MAC and IP address, interface speed, number of received / transmitted bytes and interface MTU (Maximum Transmission Unit).



Network interfaces

INTERFACE	TYPE	MAC ADDRESS	IP ADDRESS	SPEED	RX BYTES	TX BYTES	MTU
● eth0	management interface 1	00:50:56:9e:d6:dd	192.168.50.205	1000 Mb/s	682673918 (651 MB)	261790371 (249.7 MB)	1500
● eth1	management interface 2	00:50:56:9e:d1:f4		1000 Mb/s	320880 (313.4 KB)	648 (648 B)	1500
● eth2	monitoring interface	00:50:56:9e:71:11		1000 Mb/s	1084244528689 (1009.8 GB)	0	1500
● eth3	monitoring interface	00:50:56:9e:16:26		1000 Mb/s	2335699907722 (2.1 TB)	0	1500

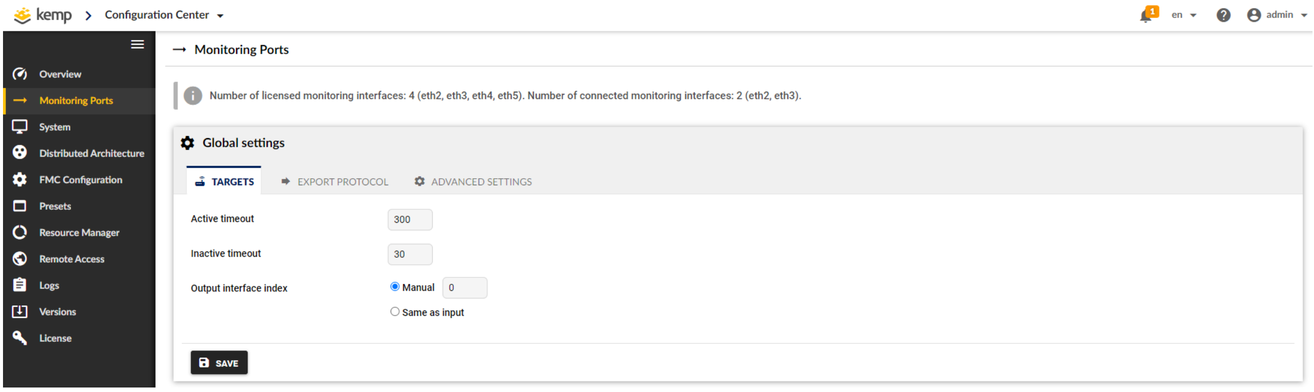
Network interfaces panel

Monitoring Ports

This panel shows the status of monitoring ports, targets and active/inactive timeouts.

Monitoring ports

This page provides the flow monitoring port management. The monitoring port is a process running over each monitoring interface. It analyzes every single received packet and computes flow statistics. The statistics are exported to a collector (e.g. Flowmon Collector or probe's built-in collector). The administrator can check the status of monitoring ports, start/stop monitoring ports or set new configuration. Each monitoring port is configured by dedicated management panel or it can be switched to the global mode in which some tabs will be configured according to the Global settings.



Number of licensed monitoring interfaces: 4 (eth2, eth3, eth4, eth5). Number of connected monitoring interfaces: 2 (eth2, eth3).

Active timeout 300

Inactive timeout 30

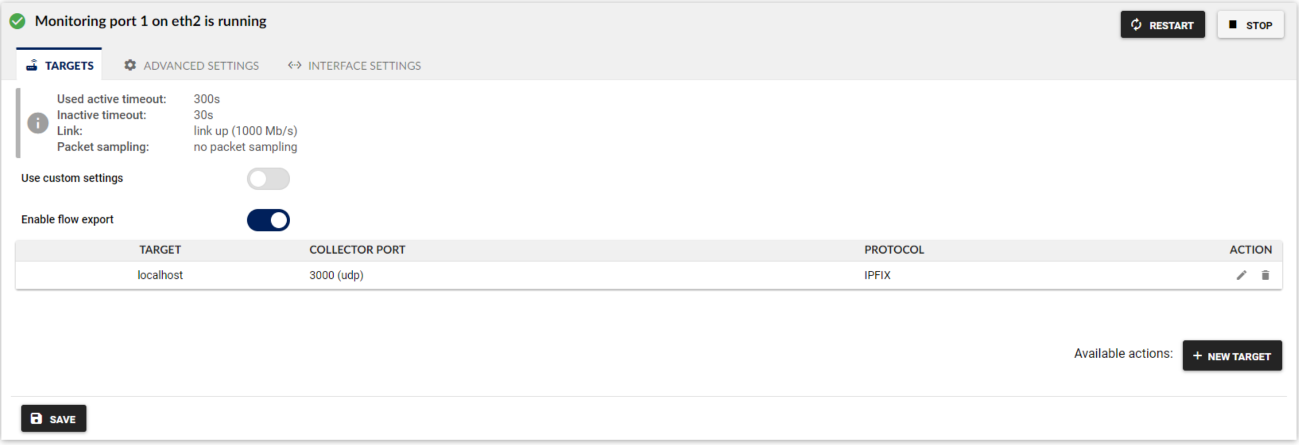
Output interface index ● Manual 0 ○ Same as input

Targets - Global Settings

Active timeout ensures that the very long flows will be exported in specified time. Timeout is checked for each incoming packet. If corresponding flow is lasting longer than specified time interval, it is deleted from the flow cache and exported to collector.

Inactive timeout avoids keeping old, inactive flow records in the flow cache forever. When no packets belonging to the flow are observed for the specified time interval, flow record is exported to collector.

The **Output interface index** is used by flow exporting routers to specify the output interface of flow. Since the probe is only receiving data, this value has no sense for it and for this reason it is filled with zero by default. However, some 3rd party collectors can consider such flows as invalid - in this case it is necessary for probe to fill this value somehow. You can configure this value manually or it can be filled automatically to the value of the input interface on which the flow was received.



Monitoring port 1 on eth2 is running

Used active timeout: 300s
Inactive timeout: 30s
Link: link up (1000 Mb/s)
Packet sampling: no packet sampling

Use custom settings ○

Enable flow export ●

TARGET	COLLECTOR PORT	PROTOCOL	ACTION
localhost	3000 (udp)	IPFIX	

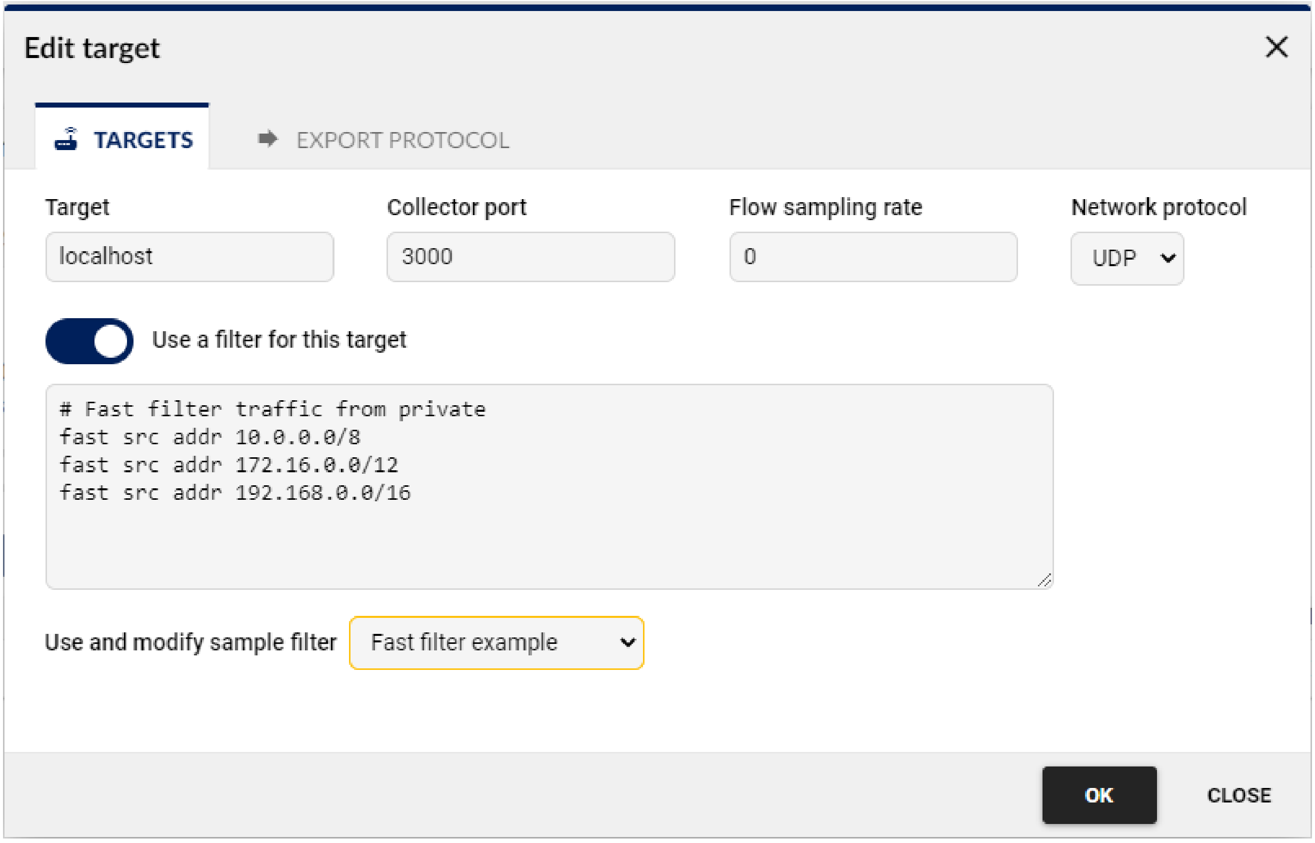
Monitoring port buttons

To start the flow monitoring port press the **Start** button. If the monitoring port starts correctly, button **Start** will change to **Stop** and button **Set Defaults** will change to **Restart** . To use default monitoring port configuration, stop it and then press **Set Defaults** button.

Targets

In the **Targets** tab you can configure various number of targets (i.e. collectors) where the flow exports are to be exported. The targets can be added or removed by pressing the **New target** or **Delete** button. Every target is specified by items **Target address** and **Collector port**. The address item is an address to a collector. If the probe built-in collector is to be used, use the address localhost. The port item specifies the listener port of the collector. For the built-in collector use the port 3000. The **Flow sampling rate** value defines a deterministic sampling (e.g sampling interval 1 in 3 flows) for monitoring port flows. If you enter a N value, every Nth flow will be exported. This is useful in situation when the collector is overloaded by incoming flows. The zero value disables this feature. The **Network protocol** option can be selected in corresponding drop-down menu. UDP (default) or TCP protocol can be selected. TCP protocol is supported for IPFIX export protocol only. If TCP is selected as network protocol, the encryption TCP/TLS can be enabled. For TCP/TLS, the set of keys and certificates have to be generated for flow exporting device (monitoring port) and for collector. All certificates must be signed by the same certification authority (CA). Its certificate (CA certificate) must be provided together with the monitoring port key and certificate to each monitoring port target using TCP/TLS protocol. The provided key(s) must not be encrypted.

By selecting **Use a filter for this target** toggle switch, you can specify filters, which will be applied for individual targets. You can write filter in the text box, pick and modify saved filter from **Use and modify sample filter** drop down menu. To apply filters, click **Ok** button. The monitoring port filter syntax is described in the section Monitoring port filter syntax.



Target: localhost

Collector port: 3000

Flow sampling rate: 0

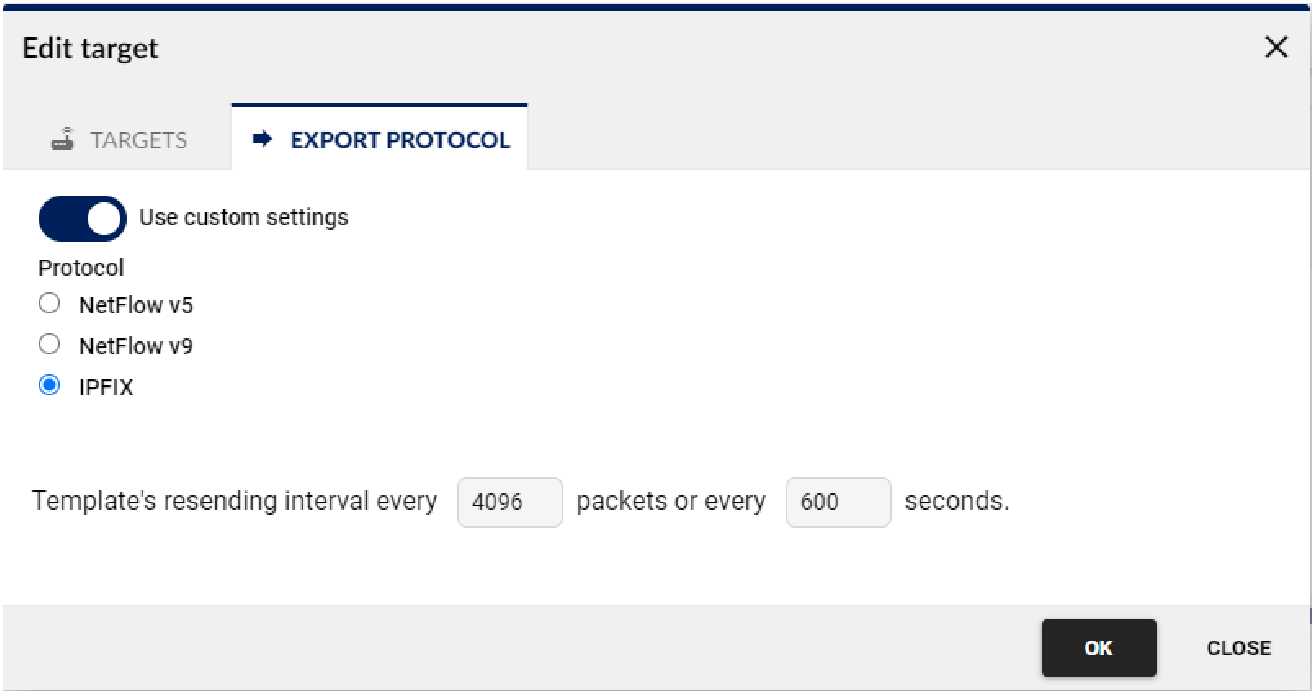
Network protocol: UDP

Use a filter for this target

```
# Fast filter traffic from private
fast src addr 10.0.0.0/8
fast src addr 172.16.0.0/12
fast src addr 192.168.0.0/16
```

Use and modify sample filter: Fast filter example

In the **Export protocol** tab you can select the Export protocol NetFlow v5, NetFlow v9 and IPFIX. By unchecking the **Use custom settings** toggle switch and clicking on button **OK** will be this tab configured according to the global configuration. Additionally, the frequency of sending the template can be configured.



Edit target

TARGETS | EXPORT PROTOCOL

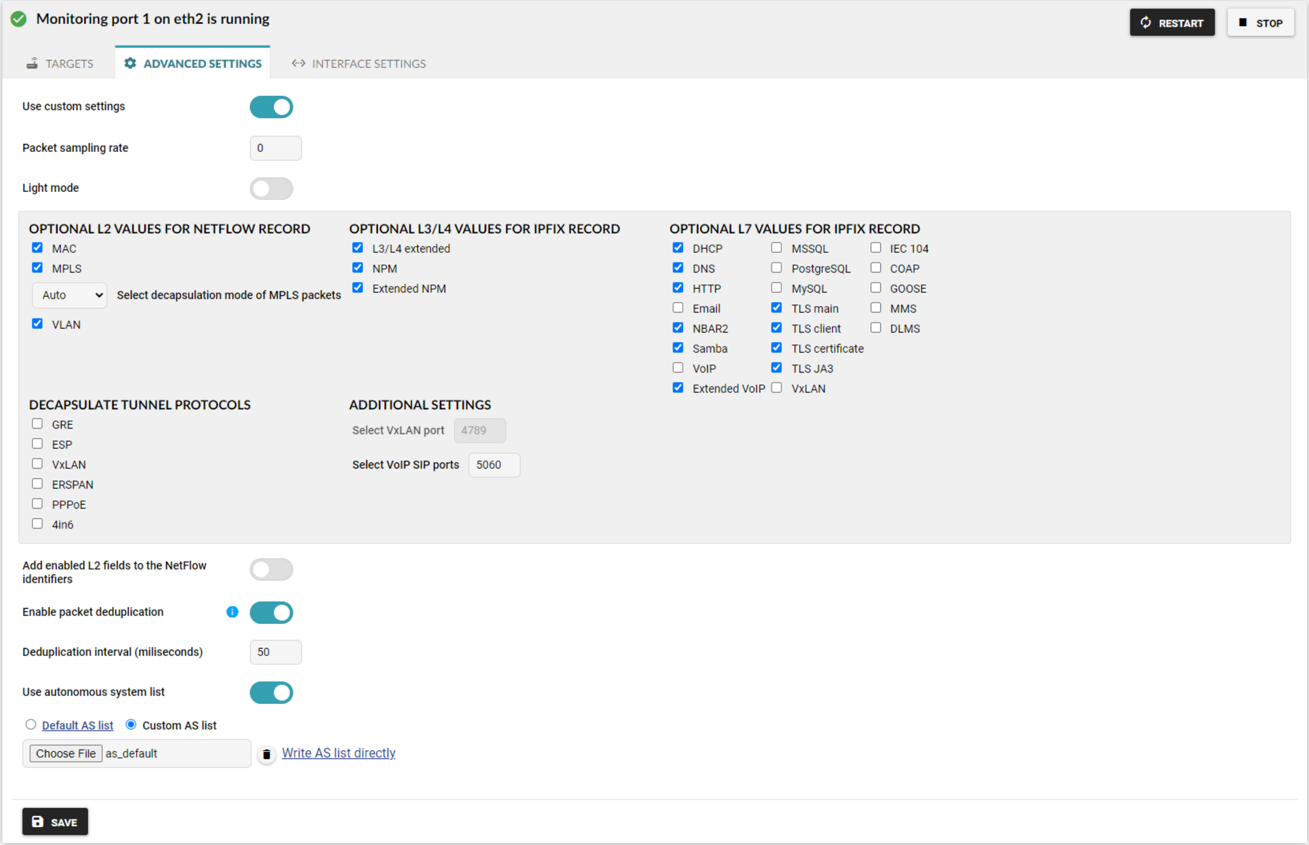
Use custom settings: on

Protocol
○ NetFlow v5
○ NetFlow v9
● IPFIX

Template's resending interval every 4096 packets or every 600 seconds.

Advanced Settings

In the **Advanced settings** tab you can configure packet sampling rate, flow identifier list and list of autonomous systems. By unchecking the **Use custom settings** toggle switch and clicking on button **Save** will be this tab configured according to the global configuration. The **Decapsulate tunnel protocols** and **Decapsulation mode of MPLS** packets options can configured here as well.



Monitoring port 1 on eth2 is running

Use custom settings: on

Packet sampling rate: 0

Light mode: off

OPTIONAL L2 VALUES FOR NETFLOW RECORD
☑ MAC
☑ MPLS
Auto — Select decapsulation mode of MPLS packets
☑ VLAN

OPTIONAL L3/L4 VALUES FOR IPFIX RECORD
☑ L3/L4 extended
☑ NPM
☑ Extended NPM

OPTIONAL L7 VALUES FOR IPFIX RECORD
☑ DHCP
☑ DNS
☑ HTTP
□ Email
☑ NBAR2
☑ Samba
□ VoIP
☑ Extended VoIP
□ MSSQL
□ PostgreSQL
□ MySQL
☑ TLS main
☑ TLS client
☑ TLS certificate
☑ TLS JA3
□ VxLAN
□ IEC 104
□ COAP
□ GOOSE
□ MMS
□ DLMS

DECAPSULATE TUNNEL PROTOCOLS
□ GRE
□ ESP
□ VxLAN
□ ERSPAN
□ PPPoE
□ 4in6

ADDITIONAL SETTINGS
Select VxLAN port: 4789
Select VoIP SIP ports: 5060

Add enabled L2 fields to the NetFlow identifiers: off

Enable packet deduplication: on

Deduplication interval (miliseconds): 50

Use autonomous system list: on

○ Default AS list ● Custom AS list

Choose File as_default — Write AS list directly

The **Packet sampling rate** defines the deterministic sampling (e.g sampling interval 1 in 3 packets) or random sampling (e.g. sampling interval 1 in 3 packets) for incoming packets. The zero value disables this feature.

Toggle switch **Light mode** can be enabled for achieving maximum performance of a monitoring port. This option is necessary for reaching wirespeed monitoring at 10Gbps and 100Gbps networks. This option disables monitoring of all additional information from L2, L3/L4 and L7 layer (only basic flow information equal to Netflow v5 including IPv6 will be monitored).

In the **Optional Lx values for NetFlow record** list, it is possible to enable monitoring of additional information from L2, L3/L4 and L7 layer.

Optional L2 values for NetFlow record

For L2, you can select monitoring of MAC, VLAN and MPLS tags (MPLS is not supported for NetFlow v5). In MPLS frames, there might be encapsulated many different kinds of protocols which are difficult to recognize as MPLS header has no information about encapsulated protocol. For this reason the encapsulated data can be selected by dropdown menu **Select decapsulation mode of MPLS packets** where either AUTO mode or specific underlying protocol can be selected. If the AUTO mode is not working properly, then try to select the underlying protocol manually.

Optional L3/L4 values for IPFIX record

For L3/L4, you can enable monitoring of extended values from L3/L4 (TCP TTL, TCP SYN packet size and TCP window size) and Network Performance Monitoring metrics (NPM - please see Network Performance Metrics paragraph below for more information). All these values are available for IPFIX protocol only.

Optional L7 values for IPFIX record

For L7, you can enable option NBAR2, which enables detection of L7 applications. Detected applications are exported by NBAR2 protocol. Next, you can enable deeper analysis of provided application protocols (e.g. HTTP, DNS, Samba, DHCP etc.). Samba protocol monitoring has some limitations - please see Monitoring of Samba protocol paragraph below. All these values are available for IPFIX protocol only.

Option TLS main

This option enables monitoring of basic information from TLS protocol. For storing the information on Flowmon collector enable extension **TLS main fields** in Flow Database Fields configuration. The monitoring functionality inspects all TCP packets and look for the TLS communication even on non-standard ports.

Option TLS client

This option enables monitoring of client specific information from TLS protocol. For storing the information on Flowmon collector enable extension **TLS client fields** in Flow Database Fields configuration. The monitoring functionality inspects all TCP packets and look for the TLS communication even on non-standard ports.

Option TLS certificate

This option enables monitoring of server certificate information from TLS protocol. For storing the information on Flowmon collector enable extension **TLS certificate fields** in Flow Database Fields configuration. The monitoring functionality inspects all TCP packets and look for the TLS communication even on non-standard ports.

Option TLS JA3

This option enables computation of JA3 fingerprint from TLS flow records. For storing the information on Flowmon collector enable extension **TLS JA3 fields** in Flow Database Fields configuration. The monitoring functionality inspects all TCP packets and look for the TLS communication even on non-standard ports.

Option VxLAN

This option enables monitoring of VxLAN VNI. For storing the information on Flowmon collector, enable the**VxLAN** extension in the Flow Database Fields configuration. If this option is enabled and the **VxLAN** option in **Decapsulate tunnel protocols** is disabled, VNI is added to the list of flow identificators (i.e. SRC IP, DST IP, SRC port, DST port, L4 protocol). This means that a new flow is created with every unique VNI. The VNI is exported in flows regardless of the configuration of VxLAN in the Decapsulate tunnel protocols section.

Options VoIP and Extended VoIP

Both options enable monitoring of Session Initiation Protocol (SIP), which is an L7 signalling protocol used in Voice over IP technology (VoIP) for initiating, modifying and terminating so-called sessions. Packet headers of SIP protocol contain information regarding initiated VoIP sessions (ID of the caller and the called party, how long the call was, whether it was initiated successfully, negotiated IP addresses and ports for Real-time Transport Protocol (RTP). SIP protocol usually works over UDP on port 5060.

The difference between VoIP and Extended VoIP is that **Extended VoIP** also attempts to match the corresponding RTP and RTCP traffic to the initiated SIP session. This allows the user to see additional information regarding RTP traffic such as audio or video codec which was used, number of transmitted bytes and packets, traffic jitter and number of lost packets. However, matching RTP traffic with SIP sessions **significantly impacts the performance** of the Flowmon Probe appliance. Therefore, it is **not recommended** to use **Extended VoIP** on appliances **where** the expected network traffic rate **exceeds 10 Gbps** per monitoring port.

These options are mutually exclusive.

Decapsulate tunnel protocols

Option ESP

This option enables ESP tunnel parsing when the ESP payload is not encrypted. Due to the protocol characteristics, it is not possible for the Flowmon Probe to conclusively decide whether the ESP payload is encrypted from the packet payload alone. Therefore, if the traffic also consists of encrypted ESP packets, it is possible that a very small portion of these packets can be misidentified, and subsequently incorrectly parsed.

Option VxLAN

This option extends the monitoring of VxLAN. The monitoring functionality inspects all UDP packets with source or destination port equal to number defined in field **Select VxLAN port**.

Option 4in6

This option enables parsing of decapsulated IPv4 network traffic transported over an IPv6 network as specified in RFC 2473 .

When option **4in6** is enabled, subsequent option **Process as DS-Lite** is shown. Enabling this subsequent option allows to analyze network traffic in the context of Dual-Stack Lite broadband deployments, as specified in RFC 6333. In such deployments, traditional 4in6 decapsulation that leads to the loss of the IPv6-related metadata is not sufficient, because the DS-Lite use-case requires unique identification of the originating Customer Premise Equipment (CPE) device (at Layer 3, this device is uniquely identified only by its IPv6 address). Therefore, it is desirable to retain the IPv6 addressing information and present it as the primary means of device identification of the collected flow data.

If the only enabled option is **4in6**, then the exported flow contains a tunneled IPv4 source and destination addresses. The IPv6 addresses are not present in the flow. If both options are enabled, then the tunneled IPv4 address is mapped to the IPv6 address as specified in RFC 4291, section 2.5.5.

L2 Fields in NetFlow

Toggle switch **Add enabled L2 fields to the NetFlow identifiers** (previously called "Add MAC address to key fields") can be used for extending the list of common flow identificators (i.e. SRC IP, DST IP, SRC port, DST port, L4 protocol) by MAC address. It can be used in special cases when you need to detect MAC address changes during communication.

Packet Deduplication

Depending on the placement of monitoring points within a network, a Flowmon Probe appliance may receive duplicated packets. The preferred way of avoiding duplicates is to select monitoring points and/or configure a traffic mirroring, TAP or SPAN in such a way that multiple copies of the same packet will not reach the Flowmon Probe appliance. If other means are not available, packet deduplication can be used to identify and remove packet duplicates directly on **Monitoring ports** of the Flowmon Probe appliance.

This option should be a last resort for removing duplicated packets that could not be dealt with by any other means. This functionality is computationally intensive and enabling it is going to negatively impact the monitoring performance of the appliance.

To start packet deduplication, switch on **Enable packet deduplication** for selected **Monitoring ports** or in **Global settings**. Every Monitoring port has its own time interval in which the packets are deduplicated. Duplicates received outside of this interval won't be detected and removed. To change this interval, use the **Deduplication interval** option. You can choose a value in the range of 1 to 1000 ms.

In **Light mode**, packet deduplication is always disabled.

To identify duplicated packets, hashes of selected packet fields are used. The hash is a combination of a flow hash and a packet hash. Flow hash is computed from typical flow identification fields such as IP addresses, port numbers and the L4 protocol number. The packet hash computation depends on the L4 protocol. For TCP, UDP and ICMP(v6) protocols the checksum field in the L4 header is used. For other protocols the whole L4 header plus 64 bytes of payload data is used.

Since the checksum field in the UDP header is optional, this field is used for hash computation only if it's value is different than 0. Otherwise the hash of an UDP packet is computed the same way as for other protocols (L4 header and 64 bytes of payload).

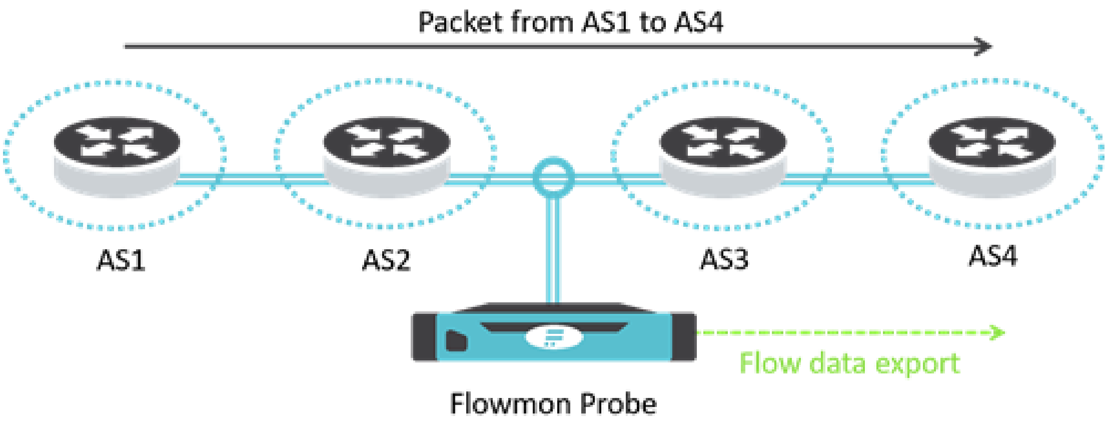
If the hash of two received packets is the same and the interval between these packets is smaller than the chosen **Deduplication interval**, the second packet is considered to be a duplicate and is removed. Packet deduplication is primarily designed for deduplicating packets in pairs, as they would arrive when both the sender and the receiver of the packet are subject to the same traffic mirroring policy. In a general use case where one packet may have more duplicates, packet deduplication will decrease the number of duplicates but it will not remove them entirely.

Enabling packet deduplication will impact Flowmon's ability to correctly detect packet retransmission rates and report issues that use this metric as an indicator. A retransmitted packet will be treated as a duplicate, if it arrives within the deduplication interval. Since packet duplication works with packets in pairs, Flowmon will be able to deduplicate and detect some retransmissions at the same time; however, the resulting packet retransmission statistics will be skewed.

Packet deduplication processes packets for every Monitoring port independently, duplicates passing through separate monitoring ports will not be detected.

Autonomous System Number Export

Flowmon Probe allows to export information concerning the source and destination autonomous systems (Origin AS method). As you can see in the following picture, while capturing packet between AS2 and AS3, the NetFlow data will contain source AS1 and destination AS4.



With the **Use autonomous system list** option you are able to apply a list of subnets for every autonomous system. The monitoring port program will then fill the AS numbers into SRC_AS and DST_AS fields of NetFlow record. If you are using NetFlow v5 export protocol, it is done automatically. If you are using NetFlow v9 export protocol, it is necessary to use a correct template containing SRC_AS and DST_AS fields.

To apply an AS list, check the **Use autonomous system list** toggle switch and choose file with list or type it manually to the text box. Press the **Save** button. If the list is wrong, monitoring port will not start and will display the error message. The AS list syntax is described in the section Autonomous system list syntax.

If you need to change the current list, simply choose the file with new list and click the **Save** button. List can be deactivated and removed by unchecking the **Use autonomous system list**.

Network Performance Metrics

Flowmon Probe is able to monitor useful metrics which can be used to measure the quality of connection. All metrics are measured in microseconds. The NPM checkbox (Network Performance Metrics) enables measuring of Round Trip Time and Server Response Time values. The NPM extended checkbox enables measuring of Jitter and Delay values. The metrics are listed below:

- **Round Trip Time** - Network delay during TCP connection establishment (so it is measured over TCP traffic only). In detail, it measures time between SYN and ACK packets, so between first and second packet sent form client. The metric is measured on flows sent from client to server only.
- **Server Response Time** - Application delay for first request for data. In detail, it measures time between request acknowledgement by server and first packet of reply. The metric is measured on flows sent from server to client.
- **Jitter** - The deviation from true periodicity of inter-packet gaps, it is measured for flows with three and more packets. In detail, it measures delay between first and second packet and then between second and third packet. The difference of these two values is Jitter. The same applies for another packets. As an output, it provides average Jitter, min, max value and standard deviation.
- **Delay** - Inter-packet delay. In detail, it subtracts packetN and packetN-1 timestamps etc. As an output, it provides average delay, min and max value and standard deviation.

Monitoring of Samba Protocol

For monitoring of Samba protocol it is highly recommended to connect probe by SPAN port, as it is required that both directions of Samba communication are monitored by the same monitoring port. If the probe is connected by tap then the information about Samba will be limited as follows:

- **Direction Client -> Server (REQUEST)**

– SMB1 command - available

– SMB2 command - available for all commands except CR and TC

– SMB2 operation - not available

– SMB2 file type - not available

– SMB2 tree path - not available

– SMB2 file path - not available

– SMB2 delete - available only if the delete was initiated by SI command

– SMB2 error - not available

• Direction Server -> Client (RESPONSE)

– SMB1 command - available

– SMB2 command - available

– SMB2 operation - mostly available

– SMB2 file type - not available

– SMB2 tree path - not available

– SMB2 file path - not available

– SMB2 delete - not available

– SMB2 error - not available

Calculation of Flowmon NPM Metrics

This chapter explains in detail how the following NPM (Network Performance Monitoring) metrics are being calculated by the Flowmon Probes:

- RTT - Round Trip Time
- SRT - Server Response Time
- RTR - Retransmissions
- OoO - Out of Order packets

All the NPM metrics are provided with microsecond precision.

Note

When specific L7 extensions are enabled, the NPM metrics are not calculated for corresponding flows. The reason is that these L7 extensions divide classic flows using additional L7 information in order to provide L7 visibility.

These smaller separate flows doesn’t contain whole communication, so the NPM statistics calculation would not be accurate. No NPM metrics (including delays and Jitter) are provided for flows with following L7 extensions enabled: COAP, SMB, VOIP, DHCP, MYSQL, PGSQL, MSSQL.

For proper NPM metrics monitoring it is necessary to have both traffic directions monitored by a single monitoring port. As a result, it is not possible to monitor NPM metrics with TAP.

Round Trip Time (RTT)

Round Trip Time represents network delay (packet going from client to server and back). It is available for TCP based network communication and measured by observing TCP handshake.

1. Server Network Time = time difference between first two packets of TCP handshake: SYN packet and SYN-ACK packet
2. Client Network Time = time difference between second and third packet of TCP handshake: SYN-ACK packet and ACK packet
3. RTT = Server Network Time + Client Network Time

Server Response Time (SRT)

Server Response Time is measured for all TCP flows and for UDP flows with DNS traffic (i.e. UDP flows where one of the ports is 53). All time measurements are done in microsecond precision.

TCP Flows

Client and server are distinguished based on who sent the SYN packet (client) and who sent the SYN+ACK packet (server). The measured Server Response Time expresses the time difference between the predicted observation time of server's ACK packet (prediction based on observation time of client request and previously measured server network time) and the observation time of server's response. The measurement can't rely on observing an ACK packet from the server before its response, since the ACK packet might be merged with the server response. If server's response packet is captured before a client's request packet, then SRT = 0.

1. If, and only if, L4 protocol is TCP, measure server network time *tsnt* as the time difference between observations of client's SYN and server's SYN+ACK packets in TCP handshake.
2.
   a. For all TCP traffic except TLS protocol: Measure the time difference Δ*trr* between first observation of server's response [(2)] and observation of the latest [(3)] preceding client's request [(1)] .
   b. For TLS protocol: Measure the time difference Δ*trr* between first observation of servers's TLS Application data response and observation of latest [(3)] preceding client's TLS Application data request.
3. Server Response Time *tsrt* = *max*(0, Δ*trr* − *tsnt*) [(4)], if Δ*trr* isn't measured at time of flow export, then *tsrt* = 0.

DNS (UDP) Flows

Client and server are distinguished based on whether 53 is the source port (server) or destination port (client). The measured Server Response Time expresses the time difference between observation times of client's request and server's response. The measurement algorithm for DNS (UDP) flows is similar to steps 2 and 3 in the TCP measurement. If server's response packet is captured before a client's request packet, then SRT = 0.

1. Measure the time difference Δ*trr* between first observation of client's request [(1)] and first subsequent observation of server's response [(2)].
2. Server Response Time *tsrt* = Δ*trr*, if Δ*trr* isn't measured at time of flow export, then *tsrt* = 0.

ⓘ **Note**

If multiple DNS requests and responses share the same UDP port number, they are processed differently. If such packets don't preserve alternating order (request, response, request, response) but they come in mixed order, the SRT is not measured.

[(1)] Any packet from client containing application layer data is recognized as a request.

[(2)] Any packet from server containing application layer data is recognized as a response.

[(3)] A client's request can contain multiple packets. In this case, use observation time of the last client's packet received.

[(4)] If the L4 protocol isn't TCP, the SYN and SYN+ACK packets were observed out of order or any of them wasn't observed, then *tsnt* is defined implicitly as *tsnt = 0*.

Retransmissions (RTR) and Out of Order packets (OoO)

Retransmissions or Out of Order packets represent situation when data packets are not correctly delivered between communication parties and needs to be resend or reassembled. Calculation is complex, explained by following algorithm.

Used terms:

- **SEQ** - sequence number of a TCP packet.
- **ACK** - acknowledgement number of a TCP packet.
- **threshold** - initial Round Trip Time (measured in TCP handshake) or 3 milliseconds (if RTT is no available).
- **TCP KEEPALIVE** - If segment length = 0 or 1 **and** current SEQ = expected SEQ - 1 **and** packet doesn't have SYN, FIN or RST flag. **Then** this packet is a TCP keepalive.
- **DUPLICATE ACK** - If segment length = 0 **and** packet doesn't have SYN, FIN or RST flag **and** window and ACK numbers are same as in previous segment **and** current SEQ = expected SEQ. **Then** this packet is a duplicate ACK.

Evaluation algorithm

Process only packets with data length > 0 or packets with SYN or FIN flag set. Skip TCP KEEPALIVE packets.

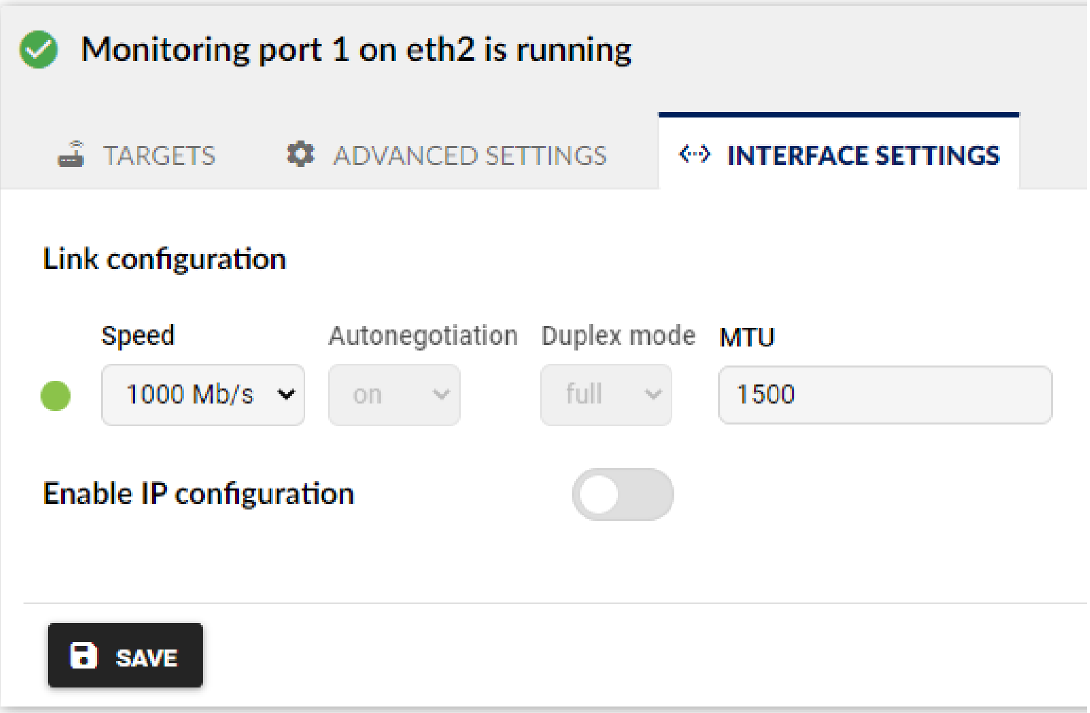
(When some of the following conditions is met, the processing of current packet ends. Conditions are executed in following order.)

- **Is it FAST RETRANSMISSION?** - If current SEQ < expected SEQ and here was more than1 DUPLICATE ACK in reverse direction (explained later) and SEQ number correspond to duplicate ACK numbers and segment was received at most 20 milliseconds after last duplicate ACK packet. Then this packet is a (fast) Retransmission.
- **Is it OUT-OF-ORDER?** - If current SEQ < expected SEQ and segment received at most "threshold" milliseconds after last segment with highest sequence number and current SEQ + segment length != expected SEQ (otherwise it would be Retransmission of last packet). Then this packet is Out of Order.
- **Is it SPURIOUS Retransmission?** - If current segment length > 0 (packet contains data) and current SEQ + segment length <= last ACK (this segment was already ACKed). Then this packet is a (spurious) Retransmission.
- **Is it RETRANSMISSION?** - If current SEQ < expected SEQ. Then this packet is a (classic) Retransmission.

Final Retransmission count is sum of all Retransmissions detected as described above.

Interface Settings

The **Interface Settings** tab allows the user to perform **Link configuration** and, optionally, **IP configuration** on the monitoring port. Configuration options provided by this tab are not available for all Flowmon models. The PRO models which are intended for monitoring of saturated 1 Gbps, 10 Gbps, 40 Gbps or 100 Gbps links do not expose this functionality. Some items in the **Link configuration** section may be unavailable on certain hardware appliances (depending on limitations of the available hardware) or certain virtualization platforms (depending on properties of the platform and/or user configuration of the environment).



Monitoring port 1 on eth2 is running

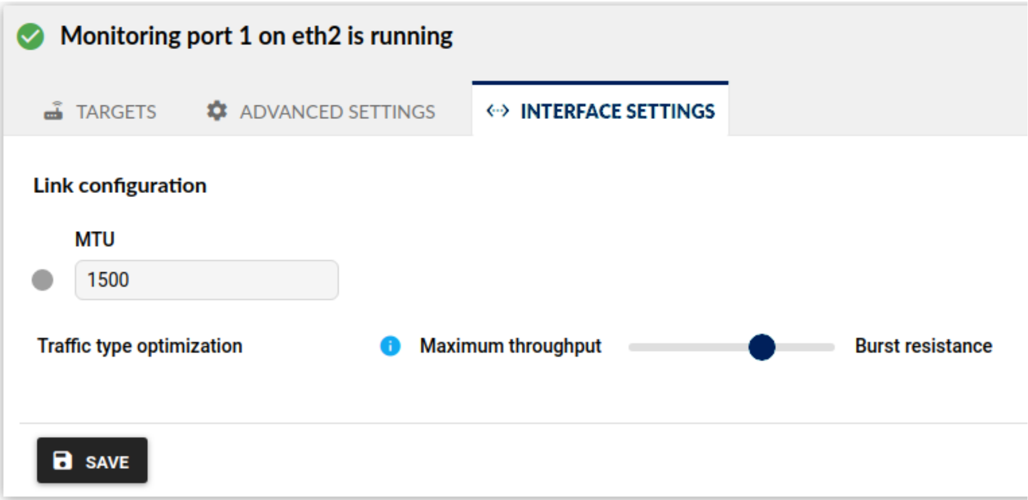
Link configuration

Speed	Autonegotiation	Duplex mode	MTU
1000 Mb/s	on	full	1500

Enable IP configuration

After enabling **IP configuration**, an **IPv4 address** and **Netmask** of the monitoring port become configurable. Optionally, **IPv6 configuration** can be enabled as well. Using the **New Static Route** button, custom static routes can be added to adjust routing for the monitoring port.

Configuration of the monitoring port on the s elected appliance models can be optimized for processing a constant stream of smaller packets (**Maximum throughput**) or for minimizing packet drop during occasional packet burst (**Burst resistance**). This configuration option represents a trade-off in which increasing burst resistance decreases the maximum throughput of the monitoring port and vice versa. It is highly sensitive to the type and character of traffic in the monitored network and should be configured accordingly on a per port basis. The default value represents the best possible configuration for most appliances and monitored networks. Changing the value of this configuration option may negatively impact the performance of your appliance and lead to an increased number of dropped packets on the affected monitoring ports.



Monitoring port 1 on eth2 is running

Link configuration

MTU
1500

Traffic type optimization: Maximum throughput — Burst resistance

Changes will be applied by the **Save** button.

Syntax

Syntax of Filter of a Monitoring port

The monitoring port's filter syntax comprises of single or multiple rules for **fast filter** and for **standard filter**. The fast filter is intended to be used for very long lists of subnets, IP addresses or intervals (e.g. filter for abroad traffic). This filter is very fast and allows the monitoring port to process thousands of rules on the fly. In the opposite, the standard filter allows complex rules in small numbers.

If you want to apply negative logic on fast filter, you can apply it globally on the whole filter by declaring "global fast not":

Negative fast filter

```
#allow all traffic except
networks below
global fast not
fast addr 192.168.3.0/24
fast addr 192.168.4.0/24
```

You can use comments in filters. They are delimited with # character and end of line. Keyword **not** may be used to invert the whole rule only (not individual parts).

The monitoring port's filter is evaluated in the same way as firewalls do. Rules of fast and standard filter are processed in descending order and they can not overlap. First must be the fast filter block followed by standard filter block (both blocks are optional). If the packet passes through the fast filter it goes to standard filter. The first matching rule stops the evaluation. The rule beginning with a keyword **not** is evaluated in the same manner as the firewall rule REJECT; rules without **not** are evaluated as the rule ACCEPT. If there is no matching rule for a packet, it is not processed. In the firewall logic it is applied a default rule REJECT ALL on the end of the list. This behavior can be changed by adding of keyword **any** on the end of the standard filter (can not be used for fast filter.) If this keyword is present, all packets that do not match any rule will be processed. In the firewall logic it is applied a default rule ACCEPT ALL on the end of the list. Result of the whole filter is evaluated as a result of logical AND of fast filter and standard filter result. If the filter is empty or no filter is given to the monitoring port, then no filtering is done and the monitoring port process all packets.

Filter Type	Syntax
Fast	**fast** [**src**|**dst**] **addr** <ip>/<mask> | <ip_start>-<ip_end> | <ip>
Standard	[**not**] [**ipproto ipv4**|**ipv6**] [[**src**|**dst**] **addr** <ip>/<mask>|<ip_start>-<ip_end>| <ip>] [**proto tcp**|**udp**|**icmp**|<number>] [[**src**|**dst**] **port** <num>|<start>-<end>] [**vlan** <number>|<start-end>]

Table 3: Filter syntax

Rule	Syntax
IP address filter	[**src**|**dst**] **addr** <ip>/<mask> | <start>-<end> |<ip>
Port filter	[**src**|**dst**] **port** <num> | <start>-<end>

Rule	Syntax
VLAN filter	**vlan** <number> | <start-end>
L4 protocol filter	**proto tcp|udp|icmp** | <number>
L3 protocol filter	**ipproto ipv4** | **ipv6**

Table 4: Standard filter rules

Standard filter examples

```
src addr 192.168.1.1-192.168.1.255 proto tcp dst port 80}
# blocks packets from
192.168.3.0/24 net to 192.168.6.0/24 net
not src addr 192.168.3.0/24 dst addr 192.168.6.0/24 addr
192.168.2.0/24 proto udp port 1-1024
dst addr 192.168.3.1
not port 80
not dst addr 192.168.3.1 dst port 80 proto icmp
src addr 2001:718::/32 dst port 42
addr 0.0.0.0/0 ipproto ipv4
addr 147.251.0.0/16
dst addr 192.168.0.0-192.168.3.42
not ipproto ipv4 src addr
192.168.3.100-192.168.3.110 proto tcp vlan 64
```

Fast filter examples

```
#allow all from networks below
fast addr 192.168.3.0/24
fast addr 192.168.255.0/24
fast addr 192.168.253.0/24
fast addr 192.168.251.0/24
fast addr 192.168.249.0/24
fast addr 192.168.247.0/24
fast addr 192.168.245.0/24
fast addr 192.168.243.0/24
fast addr 192.168.241.0/24
fast addr 192.168.239.0/24
fast addr 192.168.237.0/24
fast addr 192.168.235.0/24
fast addr 192.168.233.0/24

#and process all packets except HTTP}
not proto tcp port 80
any

# process packets from IP 1.2.3.4 except port 80.
not addr 1.2.3.4 port 80
addr 1.2.3.4
```

Negative filter example

```
#allow all traffic except networks below
global fast not
fast addr 192.168.3.0/24
fast addr 192.168.4.0/24
```

Autonomous system list syntax

Autonomous system list is defined as a list of subnet prefixes. The syntax of this filter is as follows:

Autonomous system list syntax

```
<as_num>-<ip>/<prefix>
...
```

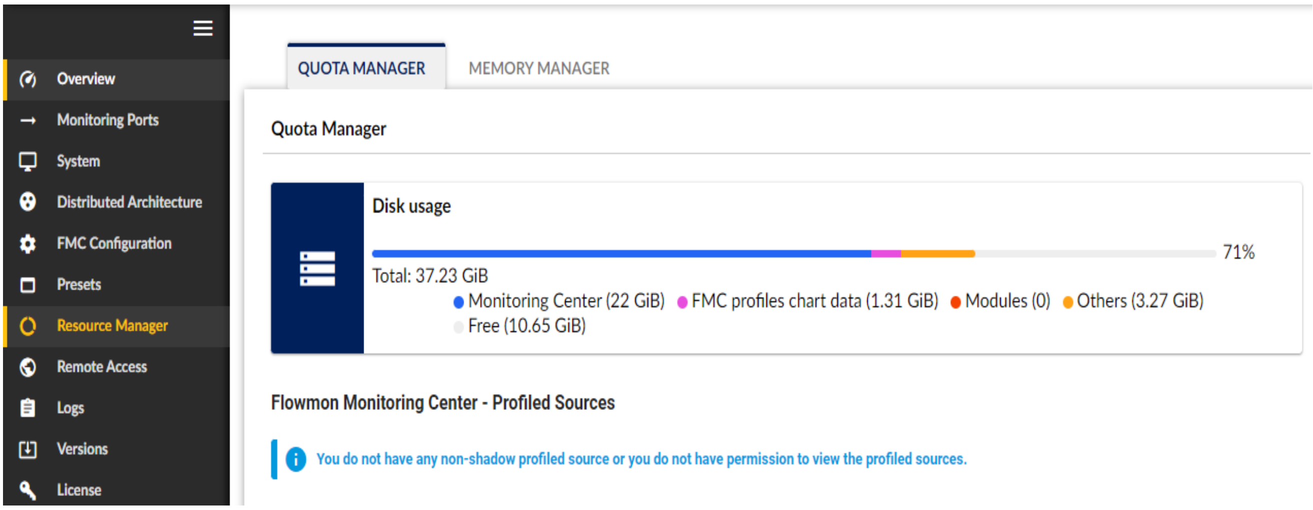
AS list example

```
15169-1.0.0.0/24
56203-1.0.4.0/22
2519-1.0.16.0/23
2519-1.0.18.0/23
2519-1.0.20.0/23
2519-1.0.22.0/23
2519-1.0.24.0/23
2519-1.0.26.0/23
2519-1.0.28.0/22
14282-2804:84::/32
28634-2804:128::/33
28634-2804:128::/32
28264-2804:130::/32
```

Resource Manager

Quota Manager

This page allows to set the maximum disk space for each module and profile from Monitoring Center. In the table you can see name, current size and maximal set quota for each record. To change the value, use slider bar on the specific line in the table or enter the value directly into the Quota field. Changes will take place after you press the **Save** button.



Quota Manager

Disk usage

71%

Total: 37.23 GiB

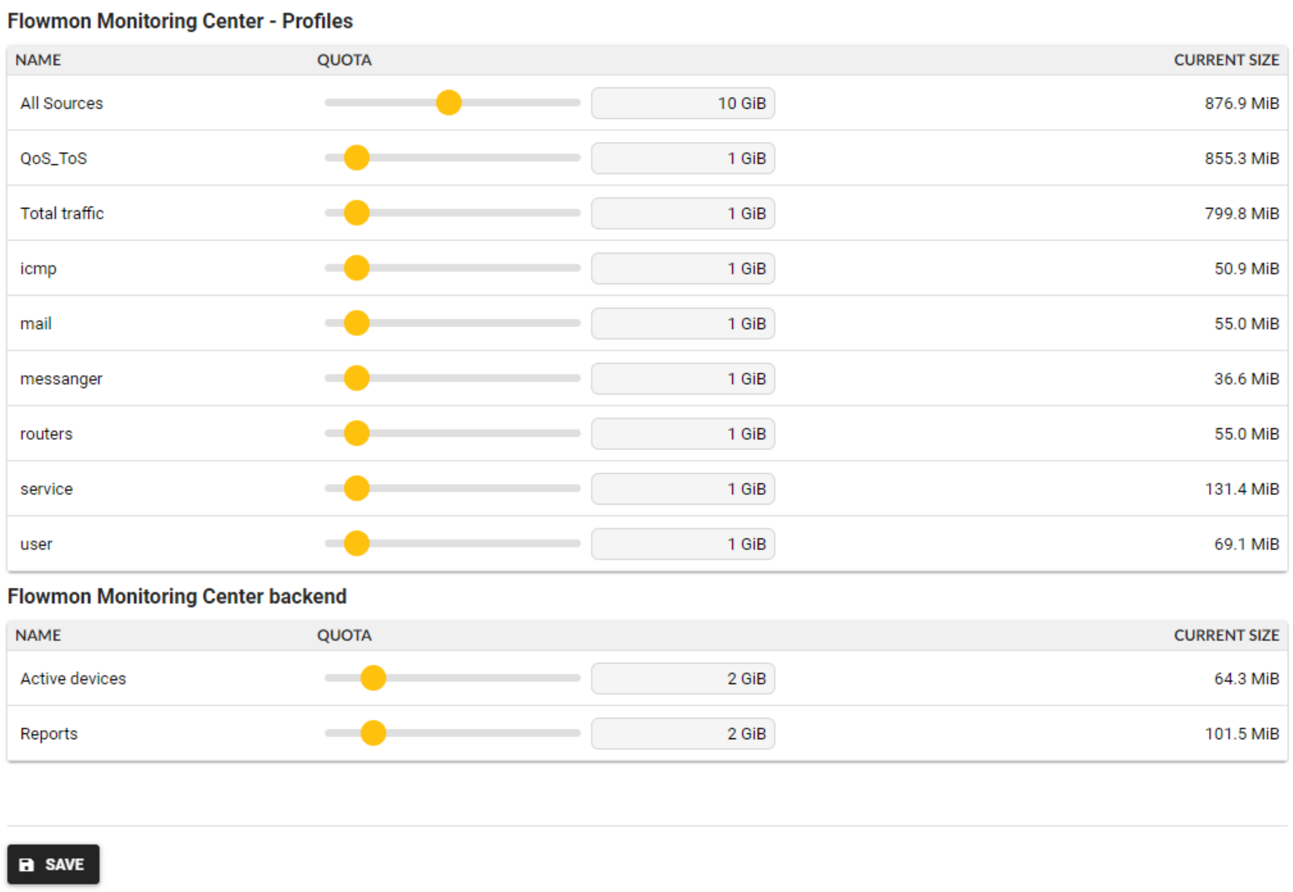
● Monitoring Center (22 GiB) ● FMC profiles chart data (1.31 GiB) ● Modules (0) ● Others (3.27 GiB)
● Free (10.65 GiB)

Flowmon Monitoring Center - Profiled Sources

You do not have any non-shadow profiled source or you do not have permission to view the profiled sources.

Warning

If you update the quota for one record via the slider, the sliders for other records are adjusted automatically. This doesn't mean that the quota were actually changed. The change of the slider indicates how much disk space can be used after the change.



Flowmon Monitoring Center - Profiles

NAME	QUOTA	CURRENT SIZE
All Sources	10 GiB	876.9 MiB
QoS_ToS	1 GiB	855.3 MiB
Total traffic	1 GiB	799.8 MiB
icmp	1 GiB	50.9 MiB
mail	1 GiB	55.0 MiB
messanger	1 GiB	36.6 MiB
routers	1 GiB	55.0 MiB
service	1 GiB	131.4 MiB
user	1 GiB	69.1 MiB

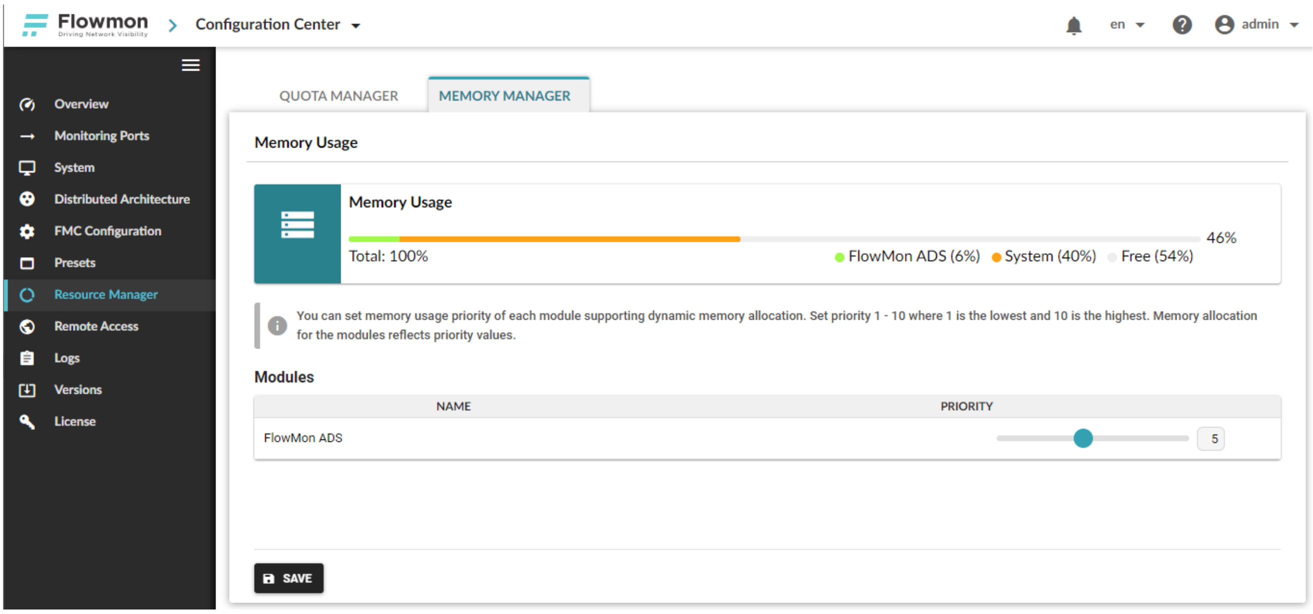
Flowmon Monitoring Center backend

NAME	QUOTA	CURRENT SIZE
Active devices	2 GiB	64.3 MiB
Reports	2 GiB	101.5 MiB

Memory Manager

This page allows to set the priority of memory usage of each module with dynamic memory allocation. The priority can be set on scale 1 - 10, where 1 is the lowest and 10 is the highest. Memory allocation ratio between individual modules reflects the configured priority values. The higher the priority the larger the memory allocated for the given module.

Changes will be applied after clicking the **Save** button.



Memory Usage

Memory Usage

46%

Total: 100% ● FlowMon ADS (6%) ● System (40%) ● Free (54%)

You can set memory usage priority of each module supporting dynamic memory allocation. Set priority 1 - 10 where 1 is the lowest and 10 is the highest. Memory allocation for the modules reflects priority values.

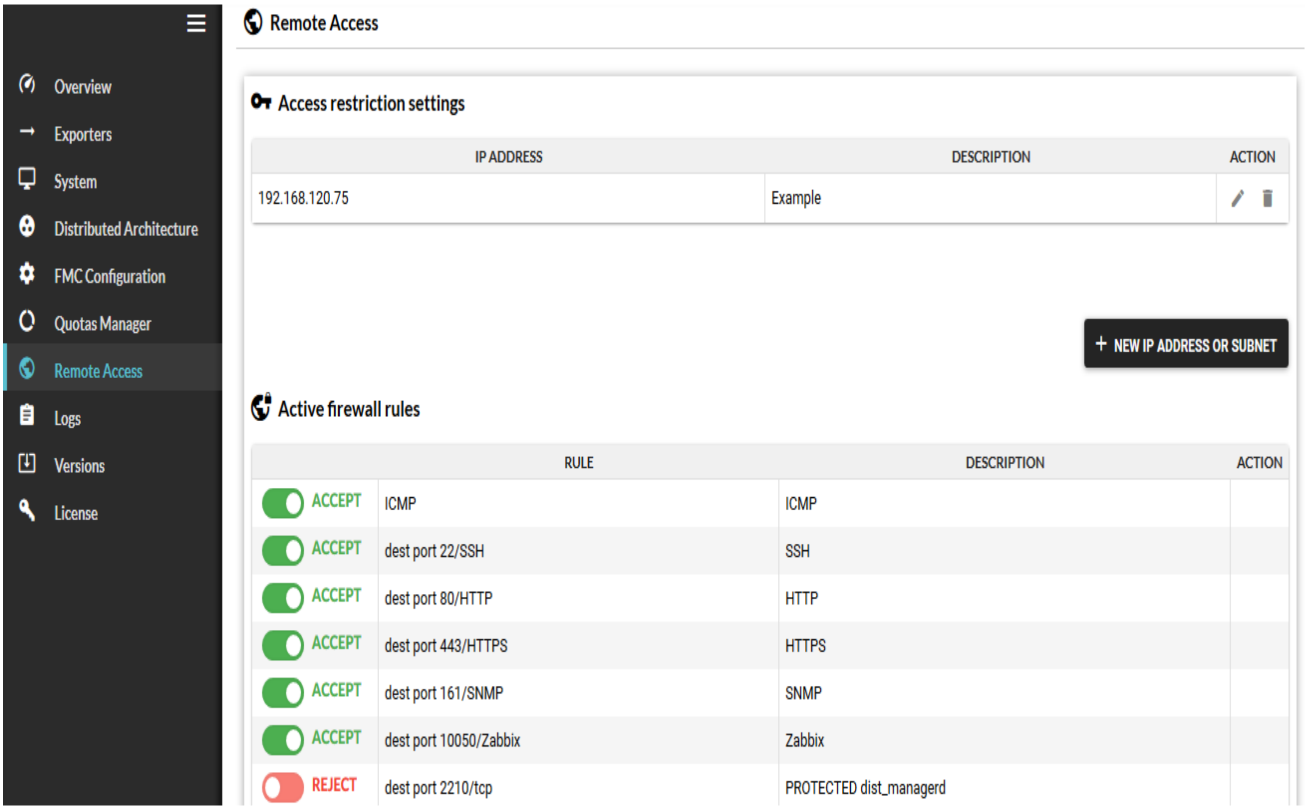
Modules

NAME	PRIORITY
FlowMon ADS	5

The setting of the priority is not available when the module is stopped.

Remote Access

On this page, there is a list of all active firewall rules and access restrictions. You may specify custom rules, which are supposed to be used for granting access to listening ports of additionally installed modules.



Remote Access

Access restriction settings

IP ADDRESS	DESCRIPTION	ACTION
192.168.120.75	Example	

Active firewall rules

	RULE	DESCRIPTION	ACTION
ACCEPT	ICMP	ICMP	
ACCEPT	dest port 22/SSH	SSH	
ACCEPT	dest port 80/HTTP	HTTP	
ACCEPT	dest port 443/HTTPS	HTTPS	
ACCEPT	dest port 161/SNMP	SNMP	
ACCEPT	dest port 10050/Zabbix	Zabbix	
REJECT	dest port 2210/tcp	PROTECTED dist_managerd	

The Remote access page

Access restriction settings

In the **Access restriction settings** panel, you can choose which IP addresses can access the Flowmon appliance via protocols **HTTP**, **HTTPS** and **SSH**. In order to be granted access to the appliance, the list of access restrictions must be empty or your host IP address must be listed or your host IP address must belong to one of the listed (sub)network IP addresses. Every access restriction entry specifies a host IP address or a (sub)network IP address that is allowed to access the Flowmon appliance. By default, these settings apply only to protocols HTTP and HTTPS. If you want to connect to the appliance via the SSH protocol, the SSH switch has to be set to ACCEPT in the **Active firewall rules** section (below) as well.

You can edit or delete restrictions using **Edit** and **Delete**. Click on **New IP address or subnet** to add a new restriction. Restricting both IPv4 and IPv6 addresses and their (sub)networks is supported.

Other protocols (ICMP, SNMP, etc.) are not affected by access restriction settings. Custom rules defined by users are also not affected by access restriction settings. Both are applied globally - to all incoming connections, based only on the configuration in **Active firewall rules**.

Active firewall rules

The **Active firewall rules** panel shows all active firewall rules. You can turn these rules and the corresponding agents on or off by toggling the **ACCEPT/REJECT** switch. The ACCEPT value means that all connection attempts meeting the rule's criteria will be allowed to pass through the firewall. The REJECT value doesn't allow such connection attempts to pass. User-defined rules always begin with the prefix **USER**. Rules beginning with the prefix **FMC source** correspond with flow sources configured on the Sources page. This prefix is followed be the name of the source.

Switches for **HTTP** and **HTTPS** are always disabled

- in state **ACCEPT** when no IP addresses are set in **Access restriction settings** or
- in state **REJECT** when one or more IP addresses are set in **Access restriction settings**.

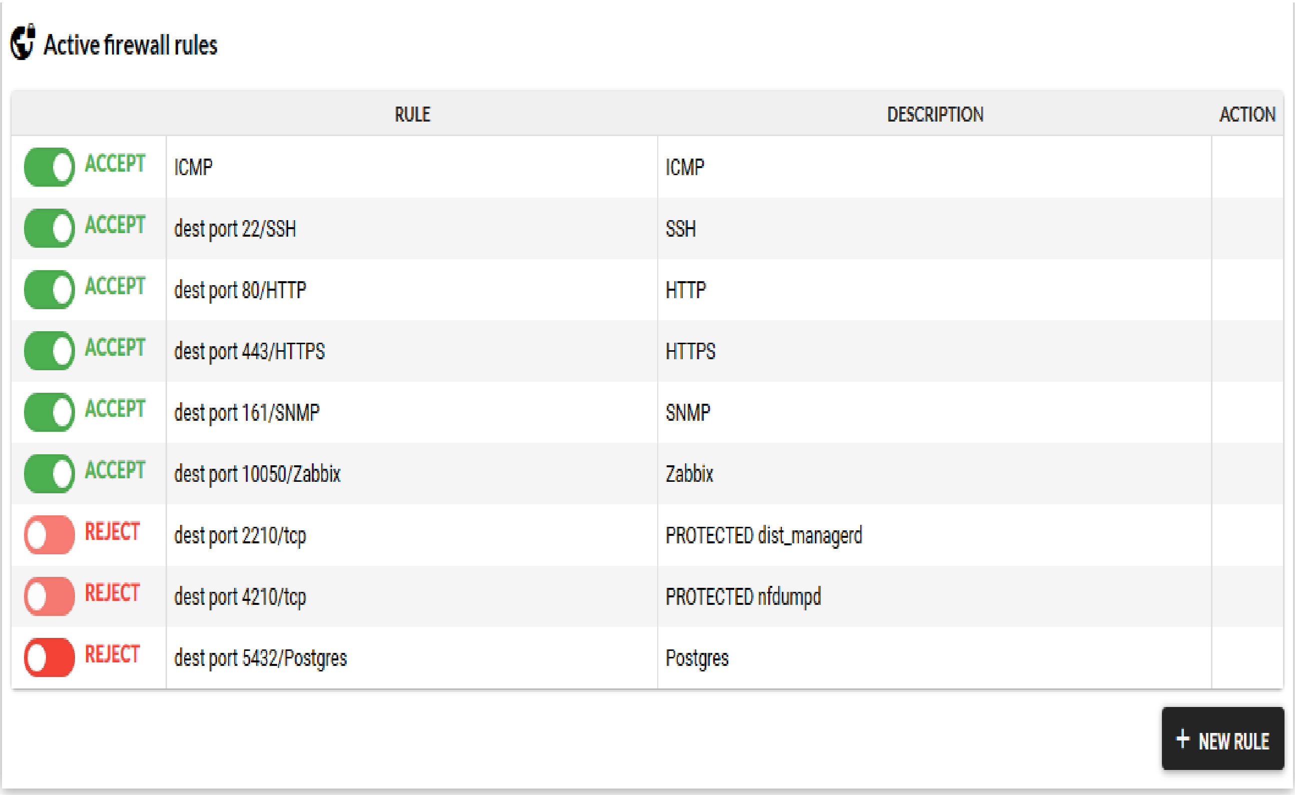
Users cannot change this configuration. The only way to control access to the appliance via HTTP and HTTPS is to set allowed addresses or ranges access restriction settings.

Switch for **SSH** is enabled and changes behavior based on the content of **Access restriction settings**

- when no IP addresses are set in **Access restriction settings**,
    - in state **ACCEPT**, all connection attempts will pass through the firewall,
    - in state **REJECT**, no connection attempts will pass through the firewall,
- when one or more IP addresses are set in **Access restriction settings**,
    - in state **ACCEPT**, connection attempts from listed IP addresses or address ranges will pass through the firewall,
    - in state **REJECT**, no connection attempts will pass through the firewall.

All other rules behave independently and do **NOT** take into account the content of **Access restriction settings**

- in state **ACCEPT**, all connection attempts will pass through the firewall or
- in state **REJECT**, no connection attempts will pass through the firewall.

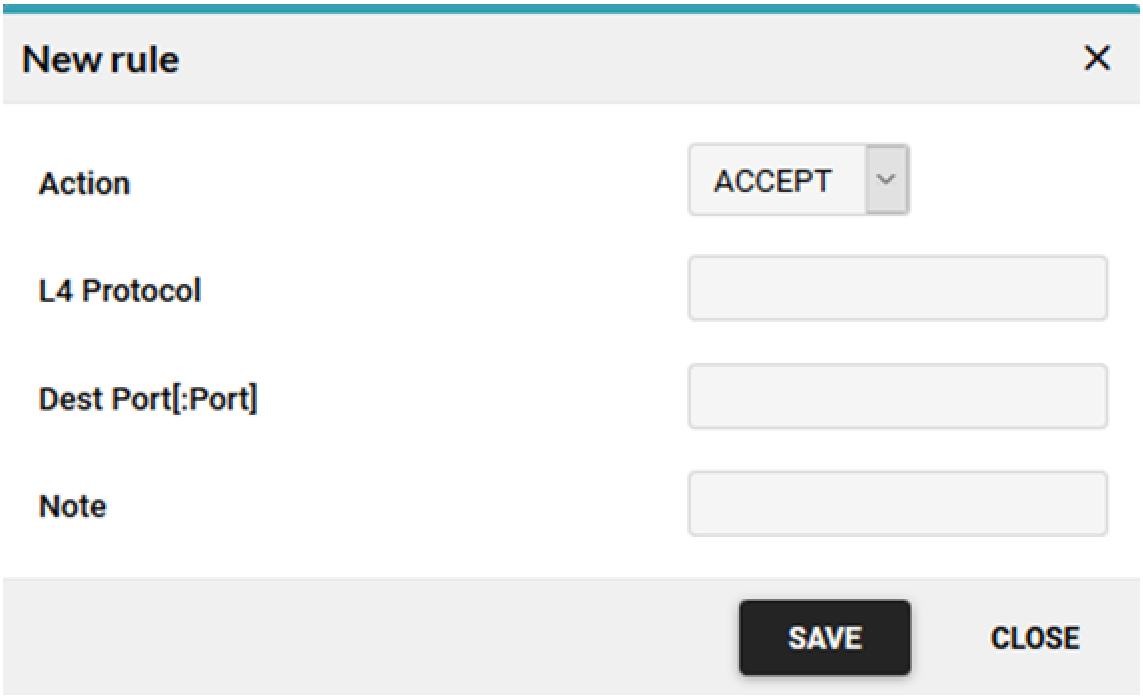


Active firewall rules

RULE		DESCRIPTION	ACTION
ACCEPT	ICMP	ICMP	
ACCEPT	dest port 22/SSH	SSH	
ACCEPT	dest port 80/HTTP	HTTP	
ACCEPT	dest port 443/HTTPS	HTTPS	
ACCEPT	dest port 161/SNMP	SNMP	
ACCEPT	dest port 10050/Zabbix	Zabbix	
REJECT	dest port 2210/tcp	PROTECTED dist_managerd	
REJECT	dest port 4210/tcp	PROTECTED nfdumpd	
REJECT	dest port 5432/Postgres	Postgres	

The Firewall rules panel

You can define your own rules and allow the listening ports of additionally installed modules by clicking on the **New rule** button. In the pop-up window, fill in the fields Action, L4 Protocol, Dest Port[:Port] and Note. The **L4 Protocol** field should be filled with the protocol code (e.g. TCP, UDP). In the **Dest Port[:Port]** field, fill in the number of the destination port. If you need to specify a port interval, type the first port number, colon and the last port number without spaces (e.g. "7000:7999"). The **Note** field is intended for the rule label.



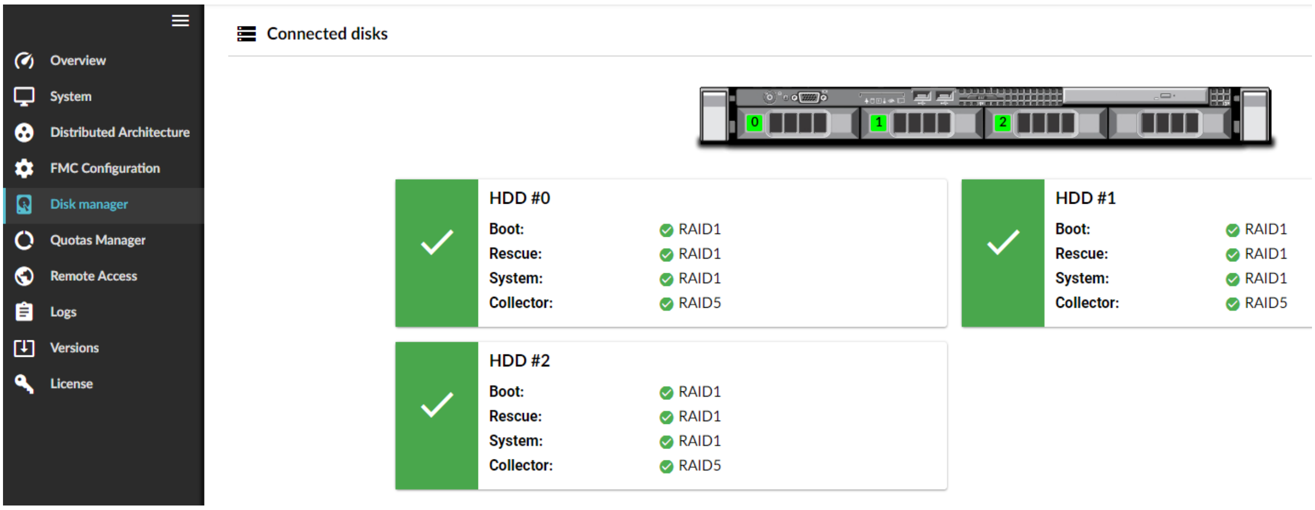
New rule

Action	ACCEPT
L4 Protocol	
Dest Port[:Port]	
Note	

The Add new rule form

Disk Management

This page is available for non-PRO models only, i.e.. collectors with SW RAID support implemented. For PRO models with HW RAID support, please use iDRAC GUI for RAID status monitoring.



HDD #0

Boot:	✓ RAID1
Rescue:	✓ RAID1
System:	✓ RAID1
Collector:	✓ RAID5

HDD #1

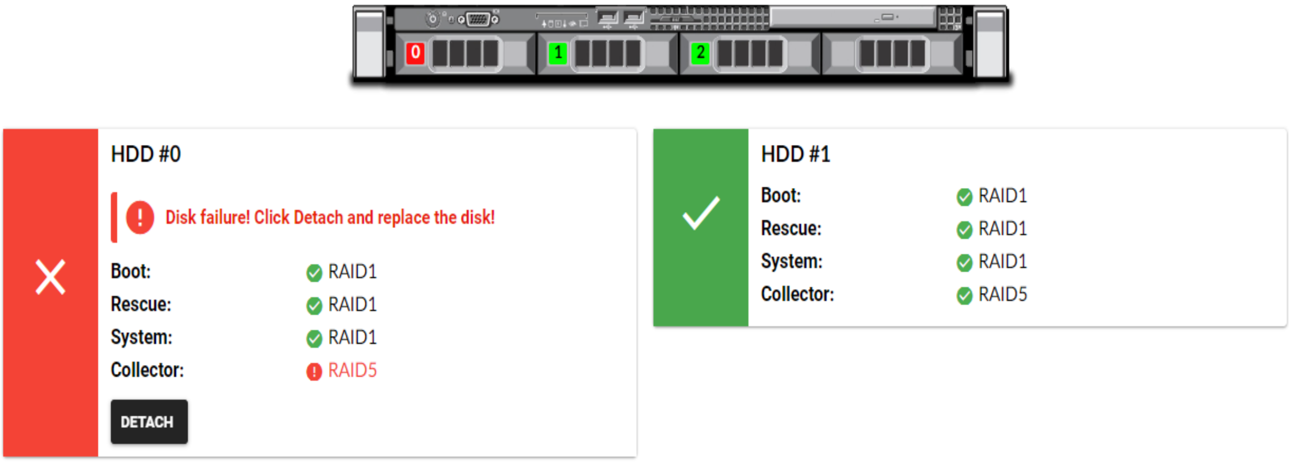
Boot:	✓ RAID1
Rescue:	✓ RAID1
System:	✓ RAID1
Collector:	✓ RAID5

HDD #2

Boot:	✓ RAID1
Rescue:	✓ RAID1
System:	✓ RAID1
Collector:	✓ RAID5

The Disk management page

In this page you can see the status of every disk partition in RAID set. If the partition is working properly, its cell contains green icon. In case of a partition failure, the corresponding cell is marked with red icon. In this case, the replacement of the failed disk should be performed as soon as possible. Prior to disk replacement it is necessary to click on the **Detach** button to detach the disk correctly from RAID set.



HDD #0

! Disk failure! Click Detach and replace the disk!

Boot:	✓ RAID1
Rescue:	✓ RAID1
System:	✓ RAID1
Collector:	! RAID5

HDD #1

Boot:	✓ RAID1
Rescue:	✓ RAID1
System:	✓ RAID1
Collector:	✓ RAID5

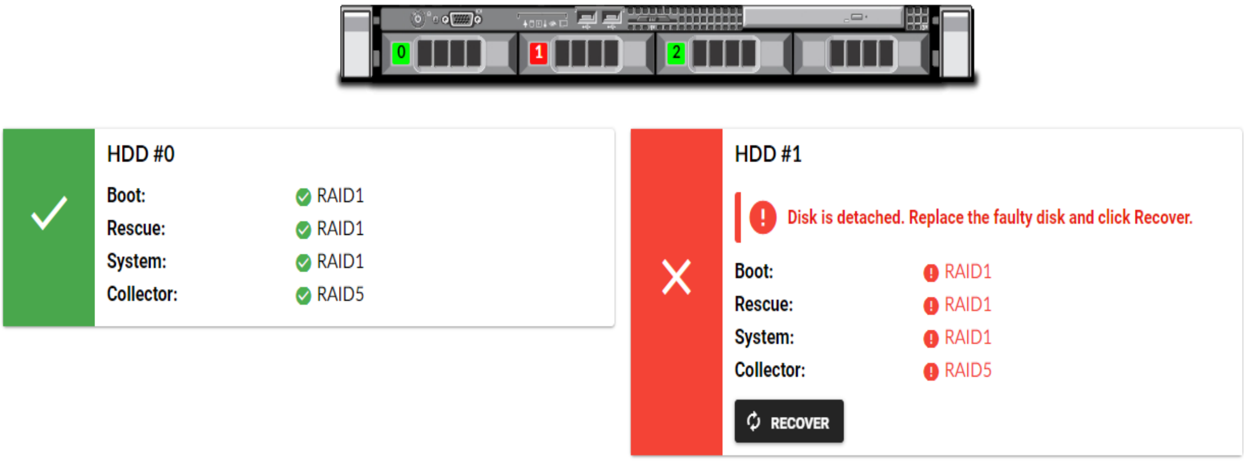
The Disk management page with failed disk

After detaching the disk, perform the disk replacement. Identify the failed disk according to its number in the HDD column in the above table (see the Identify the failed disk paragraph at end of this chapter).

Warning

If you remove a different disk instead of the failed one, all data will be destroyed irreversibly! The only way to recover the collector is by using of the Recovery CD, which resets the collector to factory settings. All data will be lost forever!

All disks in the collector are connected by hot-plug technology, so you can replace the disk during the normal collector activity. For the replacement, please use the same type of the hard disk drive, if possible. If not, use a disk, which has the same or bigger capacity than the failed one. After replacing the disk, wait for 20 seconds until the system attach the new disk and then click the **Recover** button.



HDD #0

Boot: ✓ RAID1
Rescue: ✓ RAID1
System: ✓ RAID1
Collector: ✓ RAID5

HDD #1

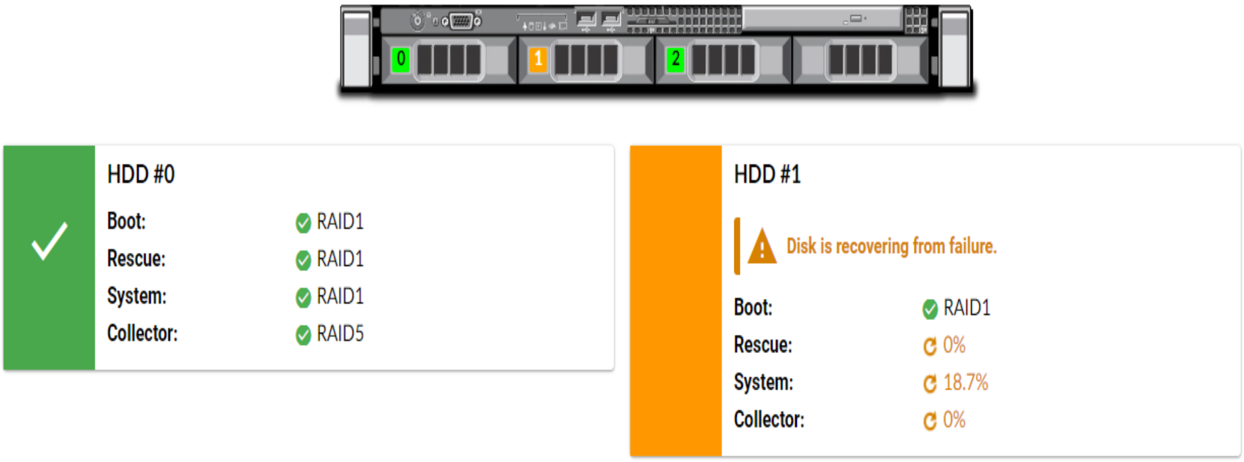
Disk is detached. Replace the faulty disk and click Recover.

Boot: ! RAID1
Rescue: ! RAID1
System: ! RAID1
Collector: ! RAID5

RECOVER

THe Disk management page with detached disk

The new disk will start to recover and synchronize with the rest of RAID set. This status is marked with a orange spinning icon followed by the percentage status. Wait, until all partitions are recovered. Beware: the replacement process is not finished successfully until the recovery process is completely finished and the green OK sign is displayed in all partitions. Until the recovery process is finished the data are not secured against failure of another disk!



HDD #0

Boot: ✓ RAID1
Rescue: ✓ RAID1
System: ✓ RAID1
Collector: ✓ RAID5

HDD #1

Disk is recovering from failure.

Boot: ✓ RAID1
Rescue: 0%
System: 18.7%
Collector: 0%

The Disk management page with disk during recovery

In case of disk failure follow the below steps:

1. Click on the Detach button in the failed disk row and wait, until the detach is finished.
2. Hot-unplug the failed disk and hot-plug the new one. Then wait for 20 seconds.

Click the Recover button.

Identify the failed disk: While looking on the front panel of the collector, the number zero disk is located on the most-left side. Going to the right, the disk numbers are increasing.

Important: While one of the disks in RAID set is failed or recovering, unplugging or failure of another disk will cause all data loss! In this case, use the Recovery CD to reset the collector to the factory settings.

Note

If the disk is unplugged without its previous detaching by the Detach button, you may not be successful to start its recovery process (after waiting for 20 seconds and pressing the Recover button, the user interface it is still not able to recognize the new disk). In this case, it is necessary to reboot your collector. After the reboot is performed, press the Recover button.

Distributed Architecture

Large and demanding network infrastructures contain many flow data sources in various locations. Processing large amounts of flow data on a single Flowmon Collector might be feasible, however this solution does not scale. In a large or expanding network the capacity of single processing unit will be eventually depleted. Distributed architecture (DA) provides high scalability and load balancing for such demanding environments. Flow data is distributed among multiple units for profiles computation and other flow data processing. More units can be simply added to increase both performance and storage capacity. Distributed Architecture provides central console for management and configuration of all units from remote geographical locations as well as data aggregation and visualization in one place.

Important information and limitations

The following list contains functionalities not yet available in current Flowmon version if **the DA is enabled**. This functionality will be enabled in future versions.

- It is not possible to backup flow data to external storage.
- Active devices are not supported when the Distributed Architecture is enabled.
- Flow forwarding is supported only on standalone Slave units.
- Channel options are not supported when the Distributed Architecture is enabled.
- No SNMP live checks of flow sources on Proxy units in DA.
- AWS Flow Logs monitoring is not supported on distributed collectors.

Following list contains important facts about DA.

- Make sure, that IP address of each unit in DA won’t be changed e.g. by DHCP protocol. If you need to change the unit’s IP address, follow instructions in chapter How to change DA unit’s IP address.

Components

There are 3 types of units in DA: **Master**, **Proxy** and **Slave units**. Master and Proxy units are dedicated hardware or virtual appliances. **Slave Units** are traditional Flowmon Collectors (hardware or virtual appliances).

Master Unit

Central console for management and configuration of other units. It provides central interface to all data from all connected Flowmon Collectors. It provides web application for data visualisation, querying, reporting and analysis. **Master Unit** gathers data from other units and assembles final result. There can be multiple instances of **Master Unit** with different priorities (the lower priority number, the higher priority of the unit). Users work with and perform configuration changes only on the top-priority instance (priority 1) called the **Top Priority Master Unit (TPM)**. Slave Units, Proxy Units and groups are configured on TPM.

TPM can initiate data queries on **Proxy Units** and obtain results. Other **Master Units** are synchronized and kept consistent with the TPM and can be set as TPM if the current TPM fails.

Master Unit requires a special license.

Note: It is highly recommended to use multiple Master Units in DA topology as a single Master Unit can’t be replaced in case of failure. If a single Master Unit fails, then with new Master Unit, the whole DA must be recreated again resulting in complete data loss on all units!

Slave Unit

Slave Units are storing and processing assigned part of flow data (see Flow Distribution Models below). More **Slave Units** can be added when needed. **Slave Units** are managed by **Proxy Units**. **Slave Units** can work in two ways as **Standalone Slave** or **Proxy Group Slave**. **Proxy Group Slave** operates as described below (Master - Proxy - Slave deployment mode). **Standalone Slave** is a **Slave Unit** which operates also as a **Proxy Unit**. In this mode there is only one **Slave Unit** in the **Proxy Group** (Master - Slave deployment mode).

Proxy Unit

Proxy Units are necessary for configurations with multiple **Slave Units** (**Proxy Group Slaves**) in one group. **Master Unit** communicates with **Proxy Units** only (to save bandwidth between different locations and for easier firewall configuration). **Proxy Unit** forwards all its requests to and from **Slave Units** in **Proxy Group**. **Proxy Unit** is used as a single target of flow export (e.g. in one geographical location) and distributes flow data to its **Slave Units**. All **Proxy Group Slaves** in **Proxy Group** must be licensed as the same collector model. For groups with single **Slave Unit** no **Proxy Unit** is needed and Slave acts as Proxy for itself (Standalone Slave).

One **Proxy Unit** and one or more **Slave Units** assigned to it creates a **Proxy Group**. Only one **Proxy Unit** is allowed in a **Proxy Group**.

Proxy Unit requires a special license.

DA unit update

Units in DA topology are all updated centrally by TPM unit. Upload the update package to TPM’s Version page. The TPM unit will perform distribution of the update package to all units in DA. The process of update is as follows:

- Update TPM unit.
- If the TPM was updated successfully, perform update on all master, proxy and standalone slave units.
- If update of proxy unit was successful, perform update of all slave units in the proxy group.

Groups

Master Group

All Master Units belongs to a group called **Master Group**. Configuration performed for **Master Group** applies to all **Master units** in DA.

Proxy Group

Proxy Unit and its **Slave Units** form a **Proxy Group**. Each **Slave Unit** can be assigned to a single **Proxy Group** only. **Proxy Group** enables scalability - if the group is overloaded, a new **Slave Unit** can be simply added to take over part of the data and tasks. Only **Proxy Groups** assigned into the **Source Group** are able to operate in the DA.

Source Group

Source Group is formed by one **Proxy Group** (mode without High Availability) or more **Proxy Groups** (High Availability mode). All **Proxy Groups** in a **Source group** are identical, deployed in the same location and receive flow data from the same flow sources (hence a **Source group**). If a failure occurs in a **Proxy Group** and DA has been deployed in the High Availability mode, data collection and query processing will not be interrupted. **Proxy Groups** are currently not able to recover missing data from other Proxy Group where the data may be available. As a result, subsequent failures in different **Proxy Groups** may lead to data unavailability or data loss.

Query Processing

Flow data is stored on **Slave Units**. **Master Unit** stores only aggregated results and metadata. Queries are initiated at **Master Unit** and forwarded to **Proxy Units**. Each **Proxy Unit** will forwards queries to its **Slave Units**. Results from **Slave Units** are aggregated by the Proxy if possible and then the results from all **Proxy Units** are sent to **Master Unit**. **Master Unit** then aggregates partial results into the final result provided to user.

Synchronization of settings among units

Flowmon Monitoring Center settings synced among **Master Group** and **Source Group units** are as follows:

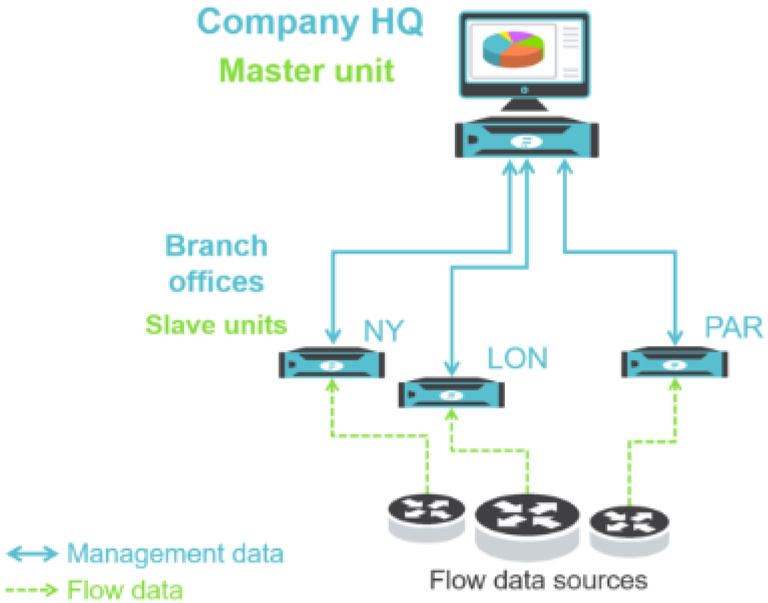
- Sources
- Profiles
- Chapters
- Alerts
- Blacklists

Flowmon Monitoring Center settings synced among **Master Group units** are as follows:

- Reports
- External reports
- Filters and Output from Advanced analysis
- renames, e.g. IP addresses

Deployment Modes

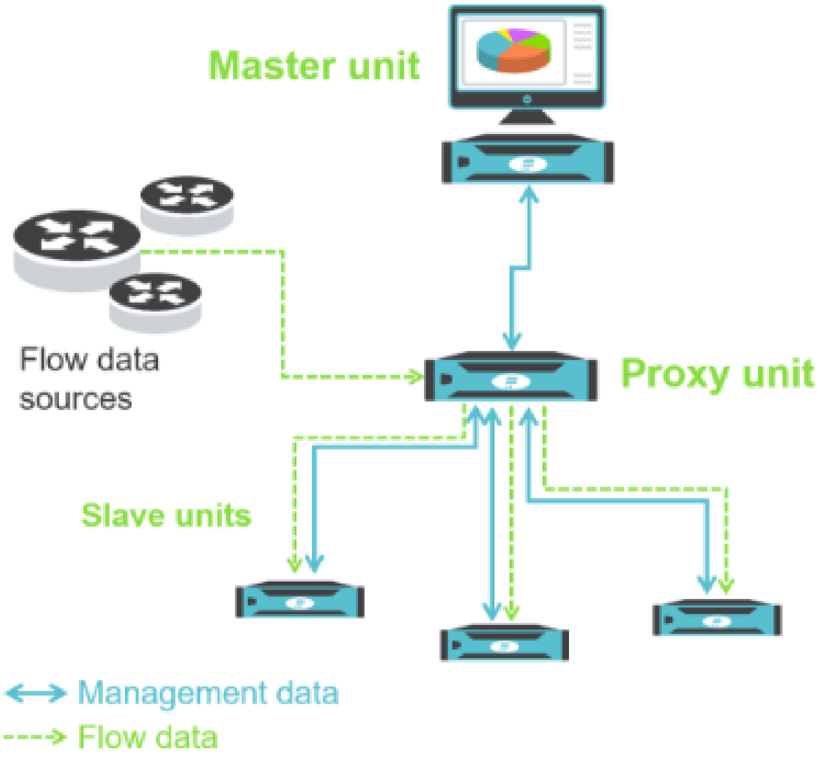
Master - Slave Mode



Master - Slave Mode

In this mode **Master Unit** communicates directly with **Slave Units** (**Standalone Slaves**). Each **Slave Unit** is set as a target of flow export for different flow data sources. In the sample diagram below, each **Slave Unit** is storing and processing flow data in the different branch office (New York, London and Paris). **Master Unit** provides central reporting and data visualization. **Slave Units** are managed by **Master Unit** from the company's HQ.

Master - Proxy - Slave Mode



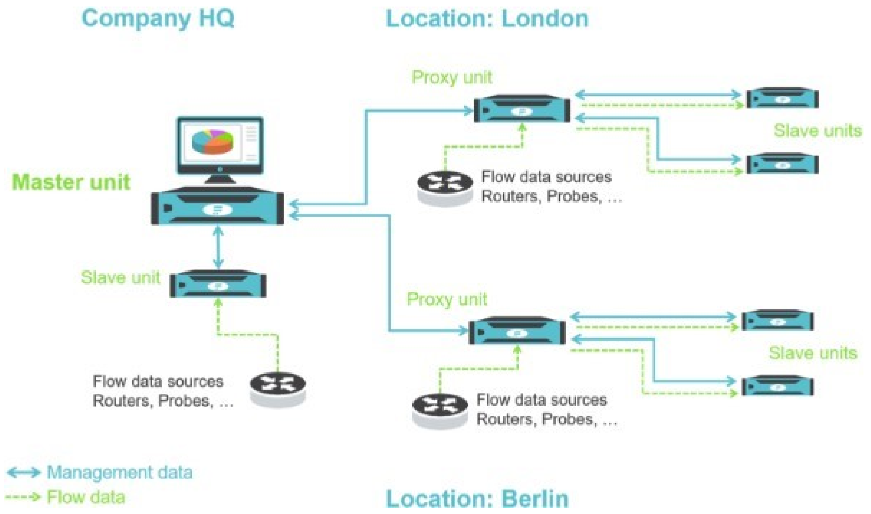
Master - Proxy - Slave Mode

In this mode **Master Unit** communicates only with **Proxy Units**. Proxy is set as a target for flow export and distributes flow data to **Slave Units** (**Proxy Group Slaves**). **Slave Units** and **Proxy Unit** form a **Proxy**

Group. **Slave Units** can be easily added to **Proxy Groups** will fully automated provisioning of all configuration needed. If multiple **Proxy Groups** are deployed into a single **Source Group** (as backup Proxy Groups for case of Proxy Unit failure), then the flow data sources must be configured to send exactly the same data to the same listening ports on all Proxy Groups.

Sample Deployment

Company headquarters is in Master - Slave mode. **Slave Unit** collects and processes data from flow data sources in HQ. Remote locations in London and Berlin are in Master - Proxy - Slave mode. **Master Unit** communicates with **Proxy Units** and it distributes flow data and configuration changes to **Slave Units**. When **Master Unit** requests data, it queries **Slave Unit** in HQ or **Proxy Units** in remote locations.



Sample Deployment

Flow Distribution Models

This chapter describes flow distribution models which are the ways how is flow data distributed among **Slave Units** in a **Proxy Group**. Models have their advantages and disadvantages.

Round-Robin Model

Every **Proxy Unit** distributes flows in round-robin manner to all **Slave Units** in its group. Incoming flow packets are de-assembled, templates are sent to all **Slaves units** and flows are distributed in round robin manner. New flow packet assembled by **Proxy Unit** must have source IP of the original flow source.

Advantages:

- Perfect scalability in group ("just add a new device to group")
- All slaves in the group are utilized equally

Disadvantages:

- More complicated data recovery *(not yet available)*

Flow Source Related Model

Every **Proxy Unit** maps flow packets from specific flow source to specific **Slave Unit** in its group. Incoming flow packets are distributed to **Slave Units** according to flow source address. Flow packets are forwarded as they are.

Advantages:

- Flows from same flow source are stored on the same **Slave Unit** - they can be used for flow source related detections etc. (e.g. anomaly detection)
- Easy data recovery *(not yet available)*

Disadvantages:

- Slaves in group are not utilized equally
- Limited scalability - flows from heavy utilized source cannot be distributed to multiple **Slave Unit**

Flow Sources Management

Each new flow source detected on **Proxy Unit** is reported to **Master Unit**. Master maps this flow source to **Source Group**, where it was detected and requests primary **Proxy Group** to obtain flow source metadata via SNMP. Flow source metadata update is requested by Master in regular manner.

Deleting flow source means to delete a channel of AllSources profile - this is automatically propagated to all sub-profiles and their channels. Delete operation is performed on Master - it will delete an AllSources profile channel (standard profile operation propagated to Proxies and Slaves) and it will also remove flow source from database and from list of flow sources of its **Source Group**. So deleting source will discard all its data in AllSources profile. In sub-profiles, the data will stay intact.

Profile Management

Profiles are managed by user on **Master Unit**. Profiles configuration remains the same as in the single system architecture. Selecting parent channels will assign each channel to specific flow sources (as each flow source is representing a root of its channel tree) and hence to a **Source Groups**. The profile is then created/modified on all **Slave Units** in selected **Source Groups**.

For Flow **Sources Related distribution model**, profile is created on all **Slave Units** in selected **Source Groups** as well, even if flow sources are not assigned to all Slaves in **Source Group**.

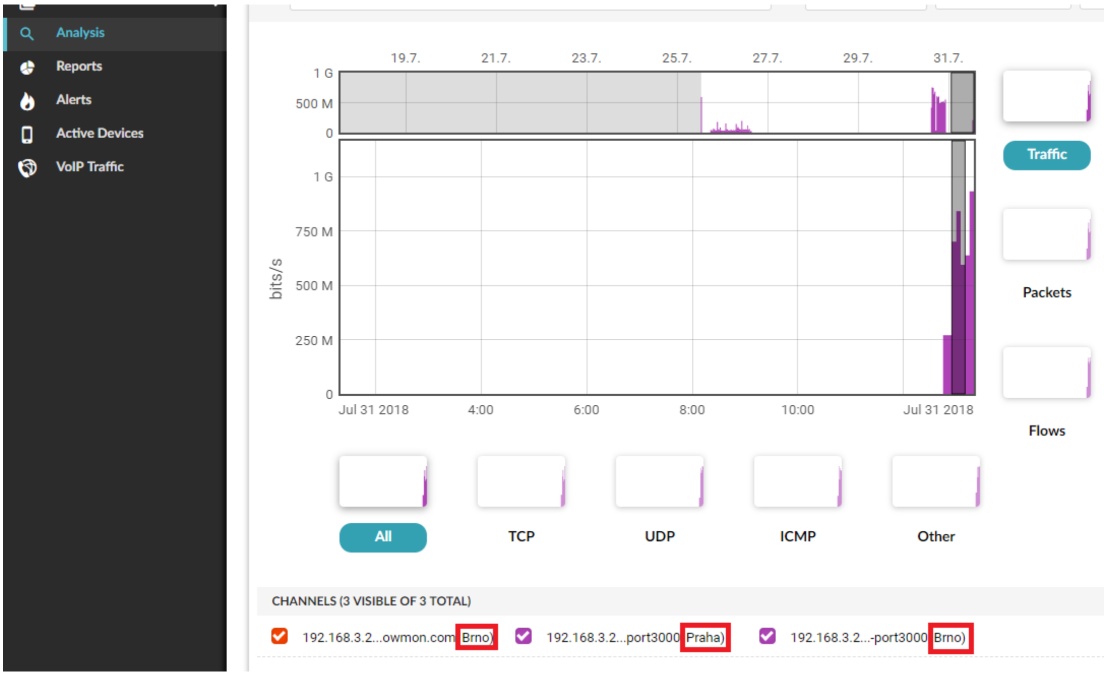
This is necessary in order to:

- keep unified configuration of all Slaves
- allow easy replacement and recovery
- allow changing list of parent channels of existing profile (subprofile of live)

When a profile is created, selected **Source Groups** then notify all **Master Units**, that the profile was created/modified. Every Slave is managing its profiles in same manner as in non-distributed architecture.

The source group(s) assigned to channel can be seen either in Analysis page in channel name or in Profiles page. See the following screenshots.

DA FMC Analysis - Channel source group (Praha, Brno)

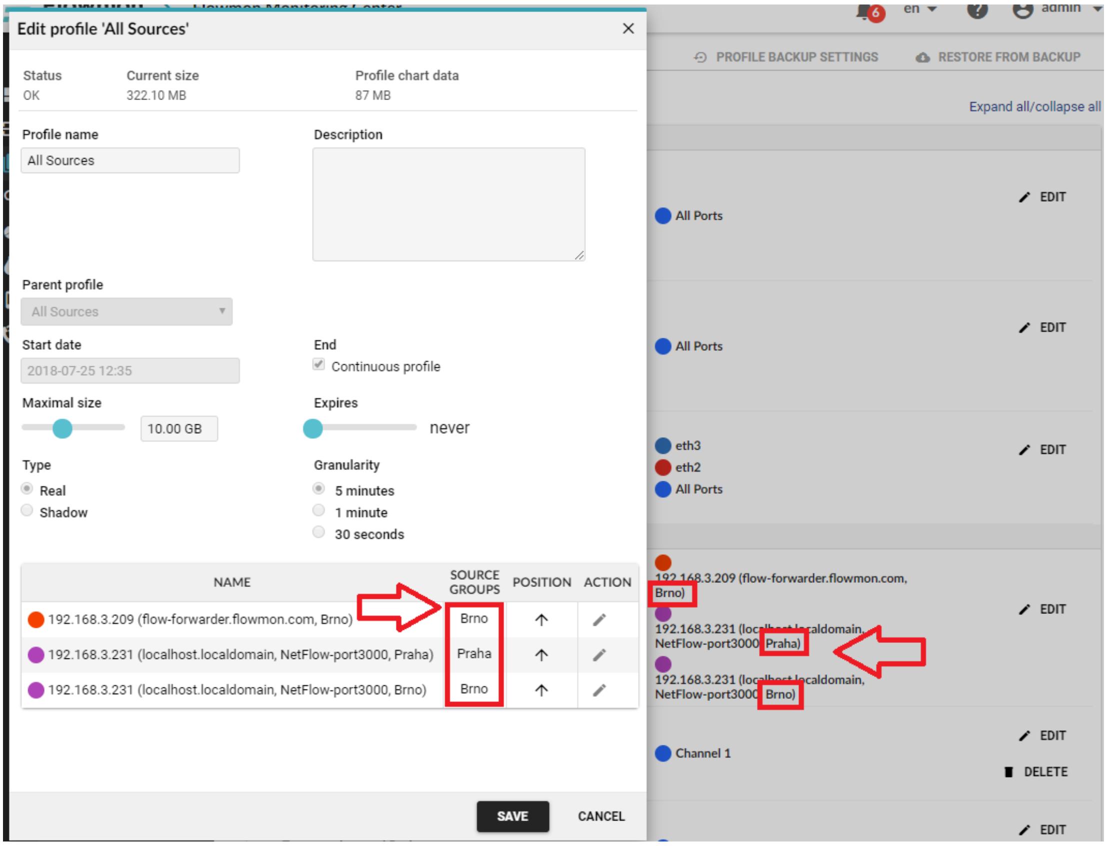


CHANNELS (3 VISIBLE OF 3 TOTAL)

☑ 192.168.3.2...owmon.com Brno) ☑ 192.168.3.2...port3000 Praha) ☑ 192.168.3.2...-port3000 Brno)

DA FMC Analysis - Channel source group (Praha, Brno)

DA FMC Profiles - Channel source group


en
admin
PROFILE BACKUP SETTINGS
RESTORE FROM BACKUP
Expand all/collapse all
EDIT
All Ports
EDIT
All Ports
EDIT
eth3
eth2
All Ports
EDIT
192.168.3.209 (flow-forwarder.flowmon.com, Brno)
192.168.3.231 (localhost.localdomain, NetFlow-port3000 Praha)
192.168.3.231 (localhost.localdomain, NetFlow-port3000 Brno)
EDIT
DELETE
Channel 1
EDIT
SAVE
CANCEL

Edit profile 'All Sources'

Status: OK
Current size: 322.10 MB
Profile chart data: 87 MB

Profile name: All Sources

Description:

Parent profile: All Sources

Start date: 2018-07-25 12:35

End: ☑ Continuous profile

Maximal size: 10.00 GB

Expires: never

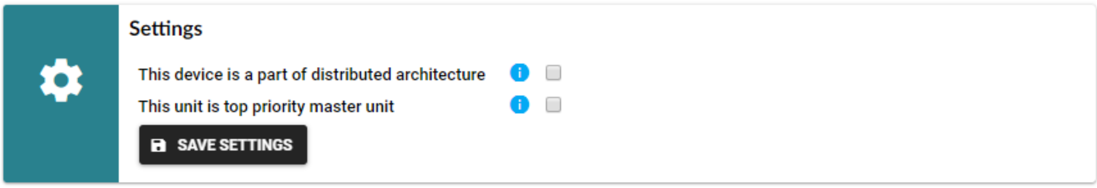
Type: ● Real ○ Shadow

Granularity: ● 5 minutes ○ 1 minute ○ 30 seconds

NAME	SOURCE GROUPS	POSITION	ACTION
192.168.3.209 (flow-forwarder.flowmon.com, Brno)	Brno	↑	✎
192.168.3.231 (localhost.localdomain, NetFlow-port3000, Praha)	Praha	↑	✎
192.168.3.231 (localhost.localdomain, NetFlow-port3000, Brno)	Brno	↑	✎

DA FMC Profiles - Channel source group

Configuration



Settings

This device is a part of distributed architecture ☐

This unit is top priority master unit ☐

DA Settings Panel

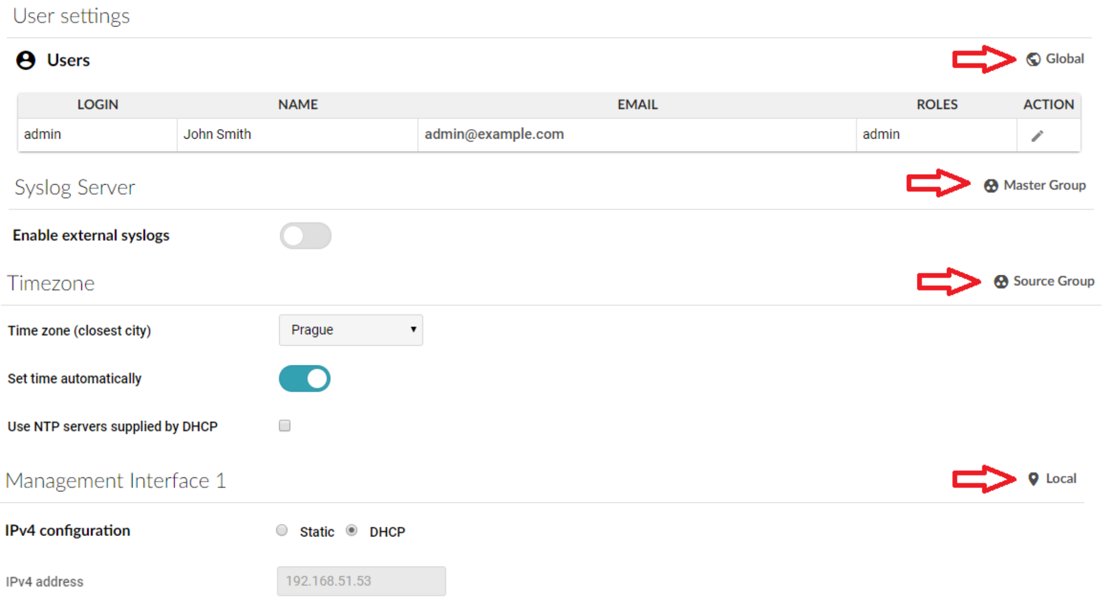
On page **Distributed Architecture** (DA) there is a panel Settings, which can be used for enabling DA feature on the box by enabling option **This device is a part of distributed architecture**. If the box is intended to work as a **Top Priority Master** (TPM), this feature must be enabled by option **This unit is top priority master unit**. Button **SAVE SETTINGS** applies the configuration.

Configuration Center on non-TPM unit

When DA is enabled on non-TPM unit, most of the configuration in Configuration Center is unavailable and must be performed via TPM.

Configuration Center on TPM unit

When DA is enabled on TPM unit, Configuration Center is available as usual. In DA mode, every configuration panel in Configuration Center is marked with one of the following indicators:



User settings

Users — Global

LOGIN	NAME	EMAIL	ROLES	ACTION
admin	John Smith	admin@example.com	admin	

Syslog Server — Master Group

Enable external syslogs: off

Timezone — Source Group

Time zone (closest city): Prague

Set time automatically: on

Use NTP servers supplied by DHCP ☐

Management Interface 1 — Local

IPv4 configuration: ○ Static ● DHCP

IPv4 address: 192.168.51.53

DA Configuration Panel Group Indicator

Their meaning is as follows:

- Global configuration - Configuration in this panel is distributed to **all units** in the distributed architecture. Global configuration panel can be configured on TPM only; on other units it is displayed in read-only mode.
- **Master group configuration** - Configuration in this panel is distributed to **all Master Units** in the distributed architecture. Master group configuration panel can be found and configured on TPM only.
- **Source group configuration** - Configuration in this panel is distributed to **all units in the Source Group**. Source group configuration panel can be found in Remote Configuration Center (RCC) of Source Group only.

- **Local configuration** - Configuration in this panel is applied to **the configured unit only**. On TPM, local configuration is changed directly in its Configuration Center. Other units must be configured via Remote Configuration Center of each unit.

DA Topology Configuration

DA topology can be configured on page **Distributed Architecture** in **Units tab**. Below Settings panel, there is a set of tables used for topology configuration. They are described in the following chapters. Every operation over DA topology is checked on TPM and TPM tries to lock all relevant Master and Proxy Units. If it is successful, the success is confirmed to user so he can continue in the work. In the meanwhile the operation is being distributed in asynchronous manner to other units in topology. The result of the asynchronous part of the operation can be checked in Action Log.

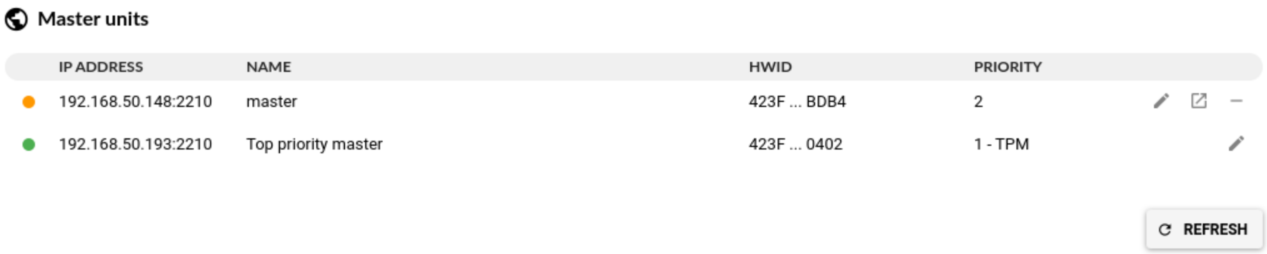
In case the topology operation cannot be performed due to check error, for the second try, the **Force** option can be selected. If the operation is forced it will most probably cause an inconsistency in your DA topology!

Warning

Before the Force option is selected, it is strongly recommended to contact Flowmon support first!

DA Topology Configuration - Master Units

Master units



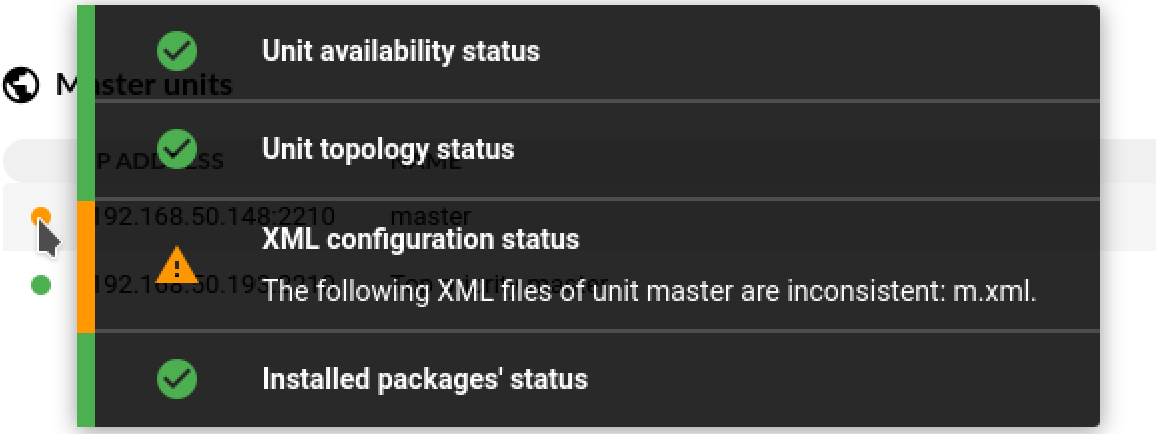
Master units

	IP ADDRESS	NAME	HWID	PRIORITY	
●	192.168.50.148:2210	master	423F ... BDB4	2	✎ ⧉ −
●	192.168.50.193:2210	Top priority master	423F ... 0402	1 - TPM	✎

In this table all **Master Units** are listed.

In **HWID column**, the HWID of the unit is displayed. To show the full HWID, the mouse has to be hovered over the HWID shortly.

Hovering the mouse over the **status icon** will display details about unit status. The status is divided into these sections:



✓ Unit availability status

✓ Unit topology status

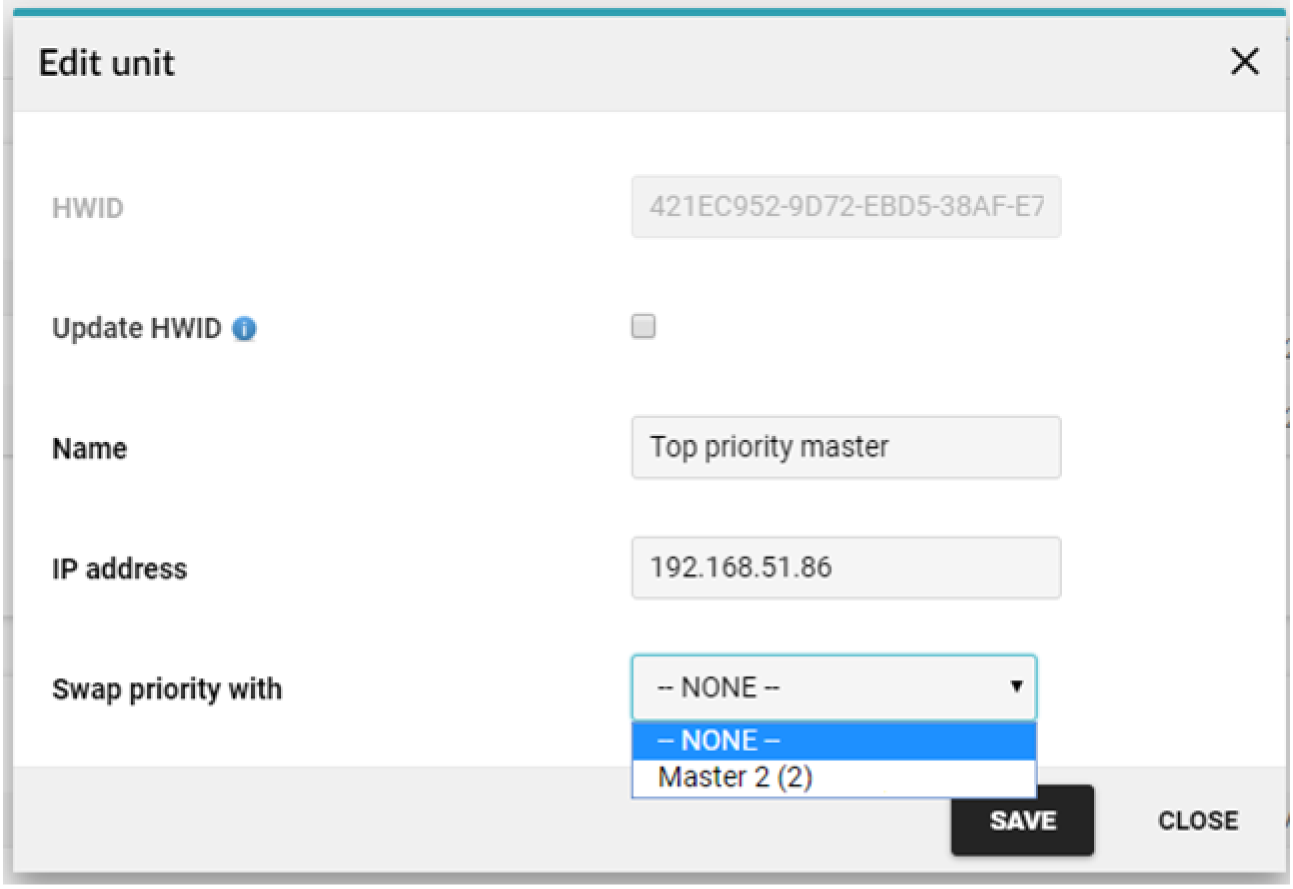
⚠ XML configuration status

The following XML files of unit master are inconsistent: m.xml.

✓ Installed packages' status

- **Unit availability status** - Indicates whether the unit is reachable within the network.
- **Unit topology status** - Indicates whether theunit is correctly embedded in the distributed architecture topology and whether it is able to utilize all its functionalities, or whether its functionalities are limited.
- **XML configuration status** - Indicates whether configuration of the unit is consistent with the TPM.
- **Installed packages' status** - Indicates whether the unit has installed packages with the same versions as the TPM.

In **Action column**, there is a button **Edit unit**. This button opens Master Unit configuration form.



Edit unit

HWID	421EC952-9D72-EBD5-38AF-E7
Update HWID	□
Name	Top priority master
IP address	192.168.51.86
Swap priority with	-- NONE -- ▾ -- NONE -- Master 2 (2)

DA Master Unit Configuration Form

In this form, following items are present:

- **Update HWID** - Each unit in DA is uniquely defined by its HWID. In an unlikely event of unit failure resulting to its complete replacement, the unit HWID in DA topology must be replaced as well. In this case it is necessary to check this option and click on SAVE button. Then new HWID is detected and unit is fully initialized with the original unit’s configuration.

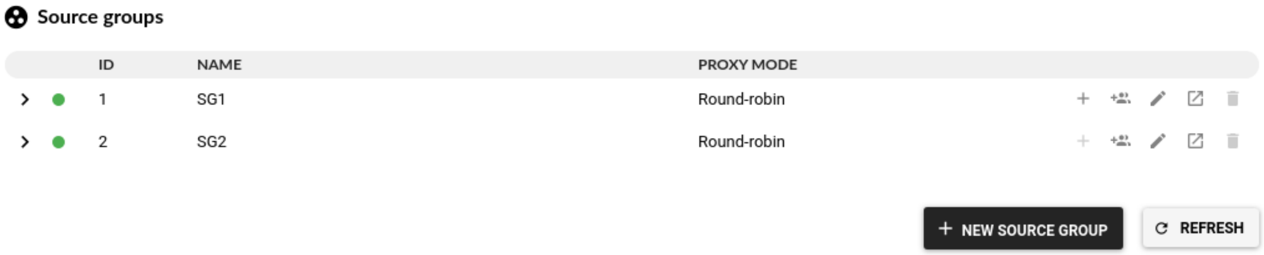
- **Name** - User defined name of the unit. Can be set to any value.
- **IP address** - IP address of the unit. For Master Unit, this IP must be reachable by users and all Master Units. For Proxy Unit, this IP must be reachable by all Master Units. For Slave Unit, this IP must be reachable by Proxy Unit from the same Proxy Group. For Unassigned Unit, the IP address must be reachable by Master Units.
- **Swap priority with** - Each Master Unit has defined priority and this option can be used for swapping priority between two Master units. If the priority is swapped with current TPM, then the second Master unit becomes a TPM after priority swap.

Next button in the **Action column** opens Remote Configuration Center (RCC) which purpose is to configure the particular Master unit. In its RCC, Local configuration can be changed. Global and Master group configuration settings can be viewed but cannot be changed.

The last button in the **Action column** removes the role assignment from the unit so it turns the Master Unit into Unassigned Unit.

DA Topology Configuration - Source Groups

Source groups table



Source groups

		ID	NAME	PROXY MODE
›	●	1	SG1	Round-robin
›	●	2	SG2	Round-robin

In this table, all **Source Groups** are listed. Each Source Group can be expanded to display all contained Proxy Groups or Standalone Slave Units. In case of Proxy Group, this can be expanded as well to display its Slave Units.

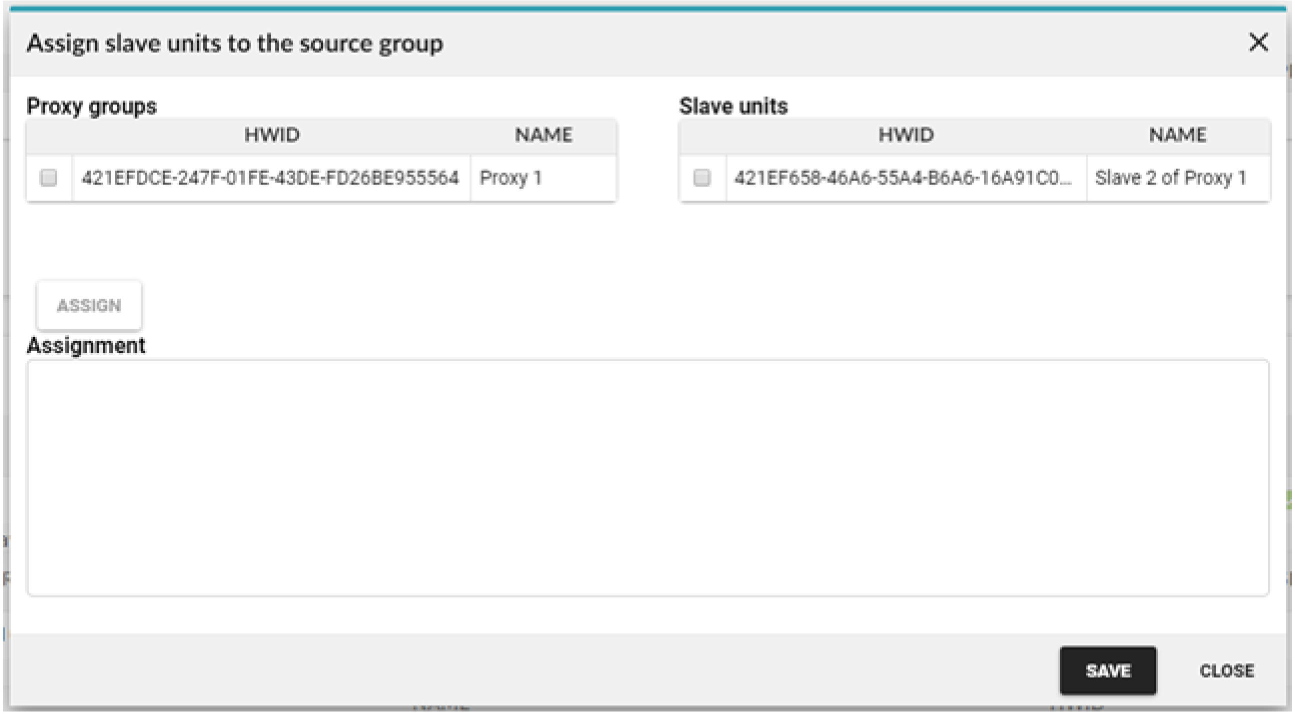
Hovering the mouse over the **status icon** will display details about unit status. The status is divided into these sections:

- **Unit availability status** - Indicates whether the unit is reachable within the network.
- **Unit topology status** - Indicates whether the unit is correctly embedded in the distributed architecture topology and whether it is able to utilize all its functionalities, or whether its functionalities are limited.
- **XML configuration status** - Indicates whether configuration of the unit is consistent with the TPM.
- **Installed packages' status** - Indicates whether the unit has installed packages with the same versions as the TPM.

Status icon for a source group aggregates status information from all its proxy and slave units.

In **Source groups** table, there is a **Action** column containing several buttons. One of them is

Assign slave units button. This button opens form **Assign slave units to the source group**.


Assign slave units to the source group

Proxy groups

	HWID	NAME
□	421EFDCE-247F-01FE-43DE-FD26BE955564	Proxy 1

Slave units

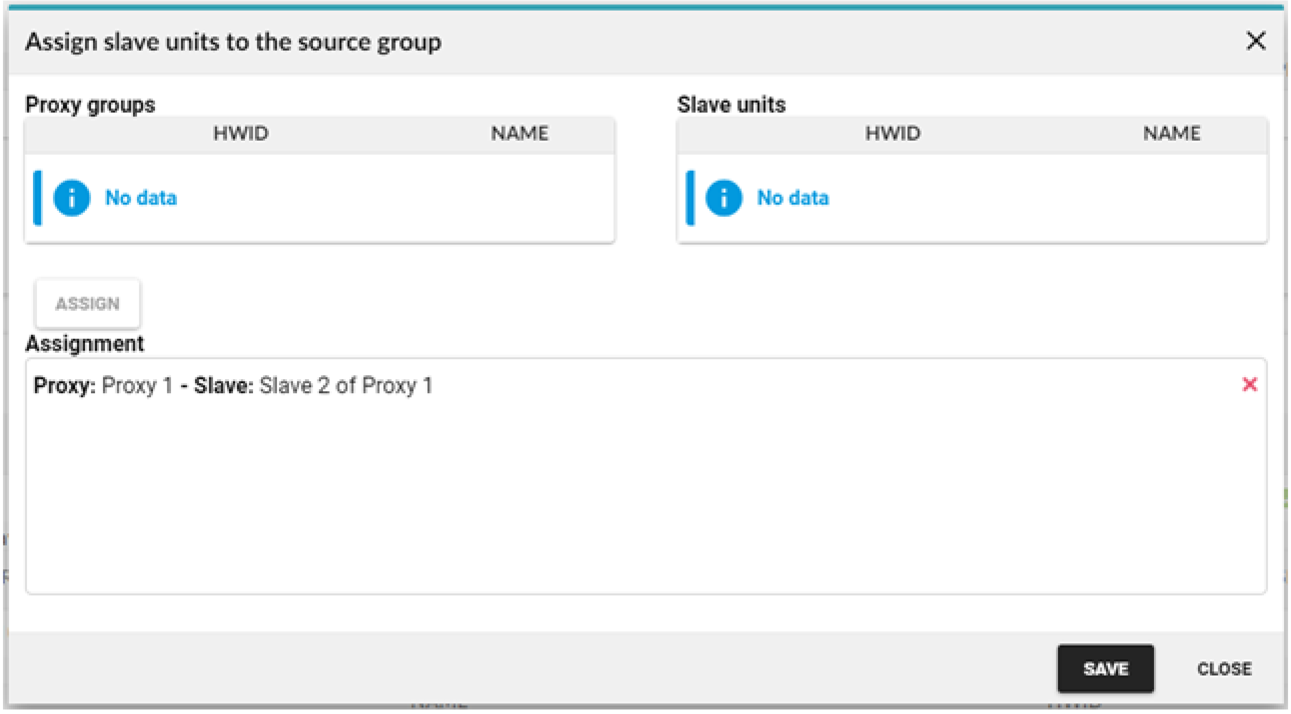
	HWID	NAME
□	421EF658-46A6-55A4-B6A6-16A91C0...	Slave 2 of Proxy 1

Assignment

DA Assign slave units to the source group

In this form, Slave Units can be assigned to all Proxy Groups in this Source Group. It is restricted that same amount of Slave Units must be assigned into every Proxy Group. All Proxy Groups in the same Source Group must have exactly the same number of Slave Units all the time.

Selected Slave Units can be assigned to selected proxy group by clicking on **ASSIGN** button. When same number of Slave Units is assigned to all Proxy Groups, the new configuration can be applied by clicking on **SAVE** button.


Assign slave units to the source group

Proxy groups

HWID	NAME
No data	

Slave units

HWID	NAME
No data	

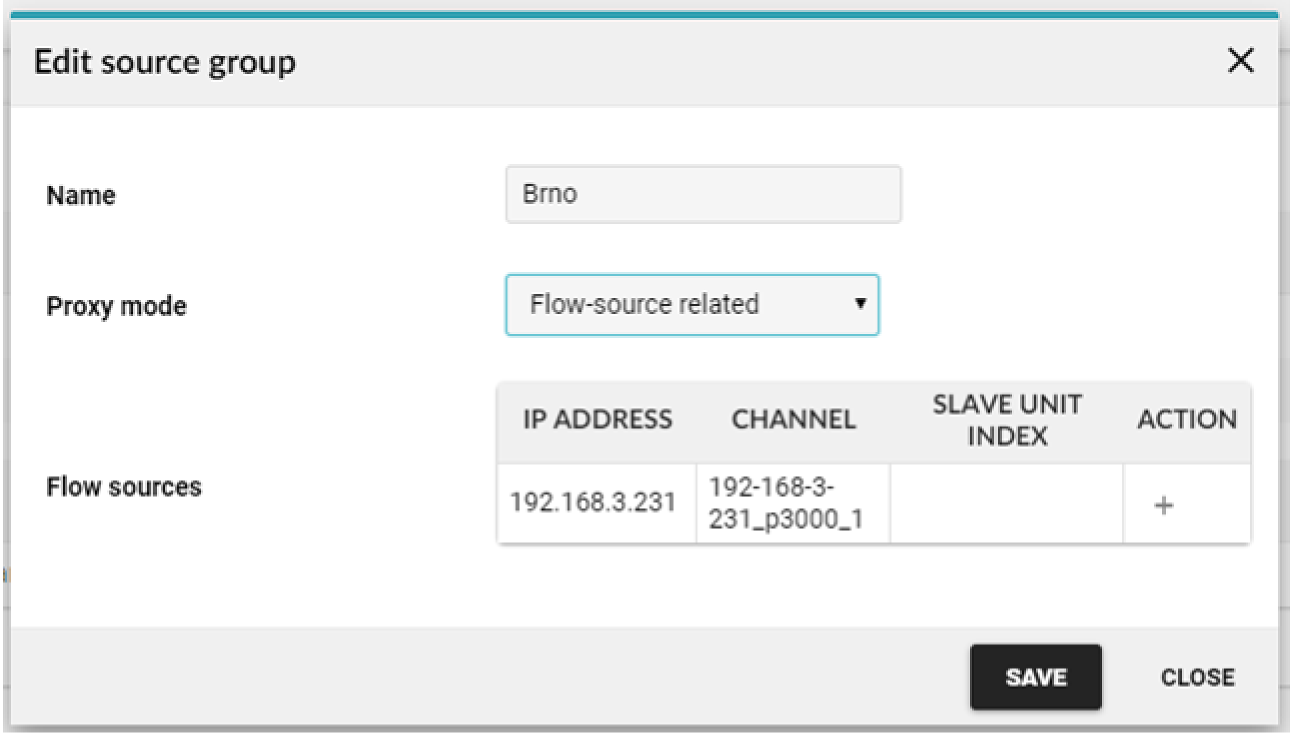
Assignment

Proxy: Proxy 1 - **Slave:** Slave 2 of Proxy 1

DA Assign slave units to the source group

Next button in the **Action column** is **Assign proxy groups or Standalone slaves** button. This button opens new form **Assign proxy groups or standalone slaves to the source group** where new proxy groups or Standalone Slave units can be added into the Source Group. Only Proxy Groups with the same number of Slave Units can be contained in Source Group.

Next button in the **Action column** is **Edit source group** button. This button opens new form **Edit source group**.



Edit source group

Name	Brno
Proxy mode	Flow-source related
Flow sources	

IP ADDRESS	CHANNEL	SLAVE UNIT INDEX	ACTION
192.168.3.231	192-168-3-231_p3000_1		+

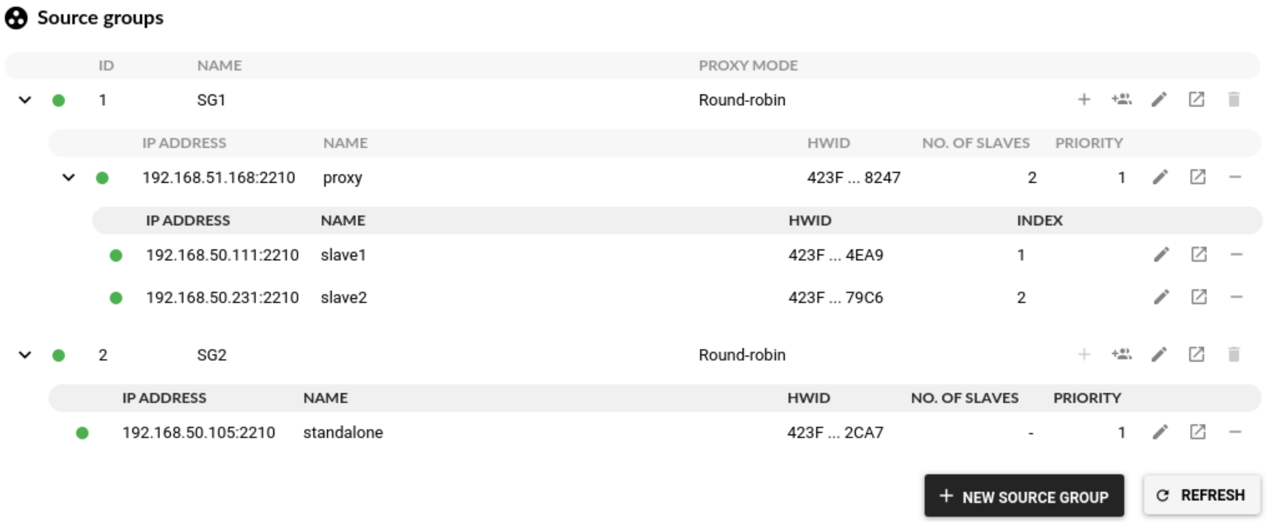
DA edit source group

In this form, **Name** of the Source Group can be set together with **Proxy mode** which can be set to **Round-robin** or **Flow-source related**. If **Flow-source related mode** is selected, then it is necessary to assign every flow source to a specific Slave Unit (multiple flow sources can be assigned to the same Slave Unit). The flows from the particular flow source will be exported to selected Slave Unit. For **Round-robin mode**, flows from all flow sources are distributed to all **Slave Units** equally.

Next button in the **Action column** opens Remote Configuration Center (RCC) which purpose is to configure the particular Source Group. In its RCC, Source group configuration can be changed. Global configuration settings can be viewed but cannot be changed.

Last button in the **Action column** deletes the Source Group. The Source Group must be empty before it can be deleted.

Proxy groups and standalone slaves table



Source groups

ID	NAME	PROXY MODE
1	SG1	Round-robin

IP ADDRESS	NAME	HWID	NO. OF SLAVES	PRIORITY
192.168.51.168:2210	proxy	423F ... 8247	2	1

IP ADDRESS	NAME	HWID	INDEX
192.168.50.111:2210	slave1	423F ... 4EA9	1
192.168.50.231:2210	slave2	423F ... 79C6	2

ID	NAME	PROXY MODE
2	SG2	Round-robin

IP ADDRESS	NAME	HWID	NO. OF SLAVES	PRIORITY
192.168.50.105:2210	standalone	423F ... 2CA7	-	1

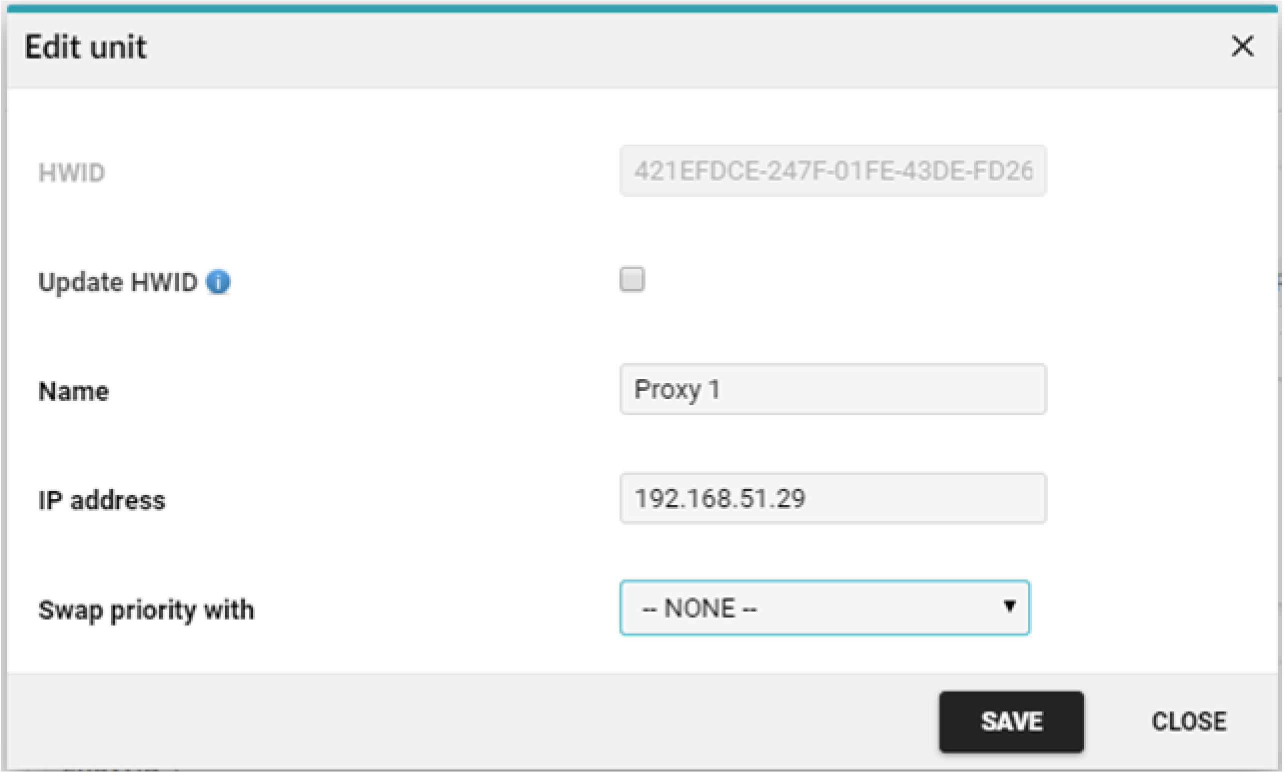
If the Source Group table is expanded, then the table of **Proxy groups and standalone slaves** is displayed showing all Proxy Groups assigned to the Source Group. Each Proxy Group can be expanded to display its Slave Units.

In **Proxy groups and standalone slaves** table, there is a **HWID column**, where the HWID of the unit is displayed. To show the full HWID, the mouse has to be hovered over the HWID shortly.

Hovering the mouse over the **status icon** will display details about unit status. The status is divided into these sections:

- **Unit availability status** - Indicates whether the unit is reachable within the network.
- **Unit topology status** - Indicates whether the unit is correctly embedded in the distributed architecture topology and whether it is able to utilize all its functionalities, or whether its functionalities are limited.
- **XML configuration status** - Indicates whether configuration of the unit is consistent with the TPM.
- **Installed packages' status** - Indicates whether the unit has installed packages with the same versions as the TPM.

In **Action column**, there is a button **Edit unit**. This button opens Unit configuration form.



Edit unit

HWID	421EFDCE-247F-01FE-43DE-FD26
Update HWID	□
Name	Proxy 1
IP address	192.168.51.29
Swap priority with	-- NONE --

Proxy Unit Configuration Form

In this form, following items are present:

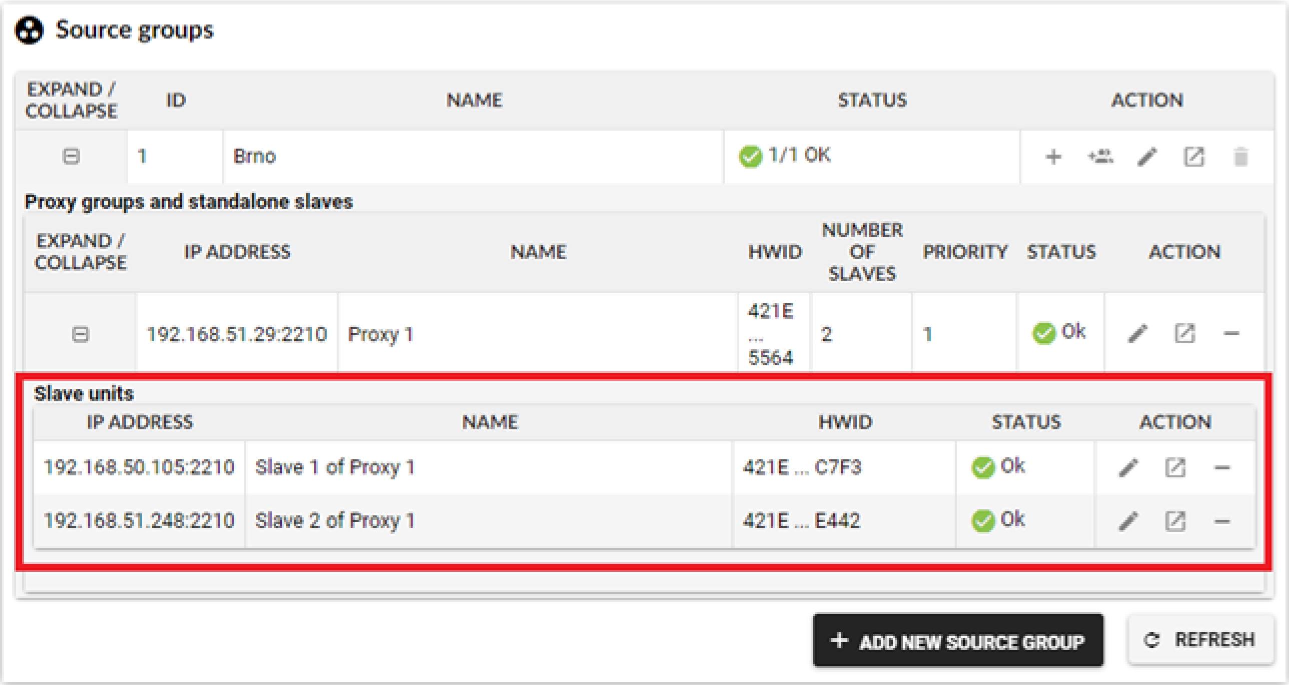
- **Update HWID** - Each unit in DA is uniquely defined by its HWID. In an unlikely event of unit failure resulting to its complete replacement, the unit HWID in DA topology must be replaced as well. In this case it is necessary to check this option and click on SAVE button. Then new HWID is detected and unit is fully initialized with the original unit’s configuration.
- **Name** - User defined name of the unit. Can be set to any value.
- **IP address** - IP address of the unit. For Master Unit, this IP must be reachable by users and all Master Units. For Proxy Unit, this IP must be reachable by all Master Units. For Slave Unit, this IP must be reachable by Proxy Unit from the same Proxy Group. For Unassigned Unit, the IP address must be reachable by Master Units.

- **Swap priority with** - Each Proxy Unit or Standalone Slave has defined priority in the scope of its Source Group. This option can be used for swapping priority between two Proxy Groups or Standalone Slaves in the same Source Group.

Next button in the **Action column** opens Remote Configuration Center (RCC) which purpose is to configure the particular Proxy or Standalone Slave unit. In its RCC, Local configuration can be changed. Global and Source group configuration settings can be viewed but cannot be changed.

The last button in the **Action column** removes the Proxy Group or Standalone Slave from the Source Group.

Slave units table



Source groups

EXPAND / COLLAPSE	ID	NAME	STATUS	ACTION
⊟	1	Brno	✓ 1/1 OK	+ ✎ ⧉ 🗑

Proxy groups and standalone slaves

EXPAND / COLLAPSE	IP ADDRESS	NAME	HWID	NUMBER OF SLAVES	PRIORITY	STATUS	ACTION
⊟	192.168.51.29:2210	Proxy 1	421E ... 5564	2	1	✓ Ok	✎ ⧉ −

Slave units

IP ADDRESS	NAME	HWID	STATUS	ACTION
192.168.50.105:2210	Slave 1 of Proxy 1	421E ... C7F3	✓ Ok	✎ ⧉ −
192.168.51.248:2210	Slave 2 of Proxy 1	421E ... E442	✓ Ok	✎ ⧉ −

DA Source Groups Table - Slave units part

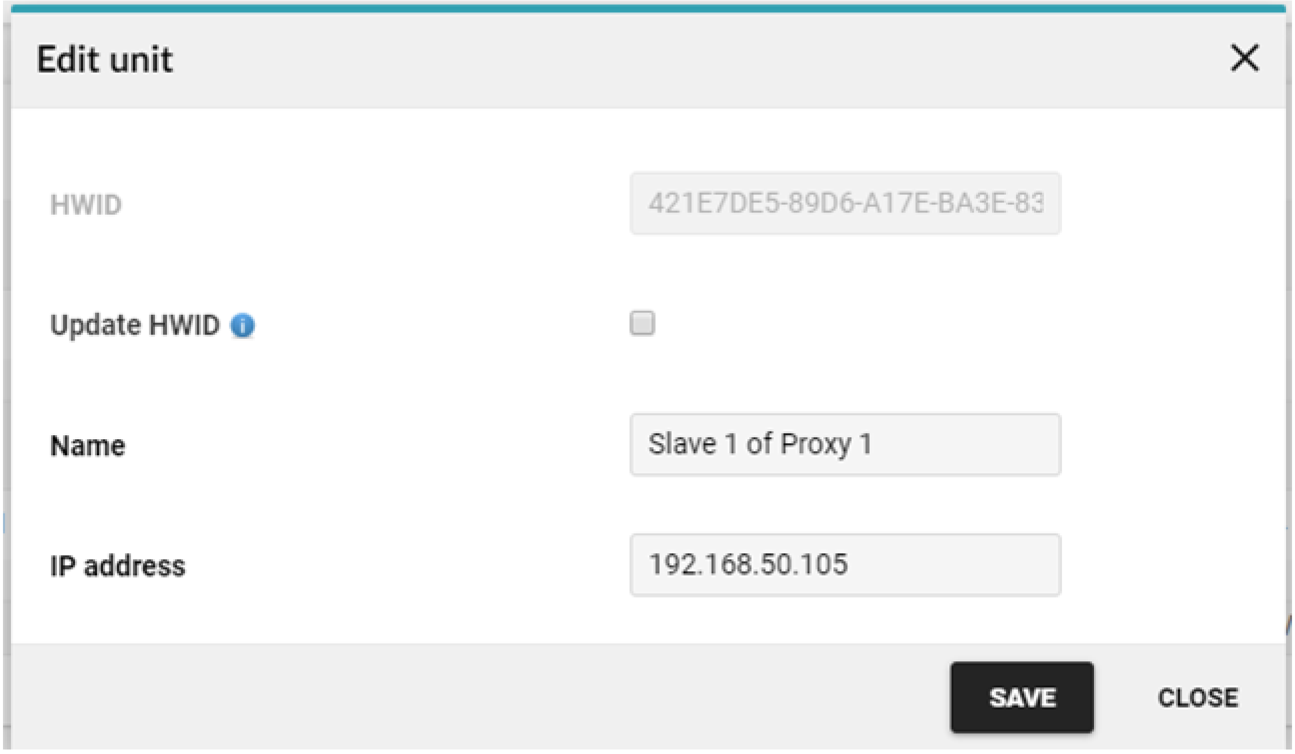
If the Proxy groups and standalone slaves table is expanded, then the table of **Slave units** is displayed showing all Slave Units assigned to the Proxy Group.

In **Slave units** table, there is a **HWID column**, where the HWID of the unit is displayed. To show the full HWID, the mouse has to be hovered over the HWID shortly.

In **Status column**, the current status is displayed. The status can be set as follows

- OK - Slave Unit is working properly
- Init - Slave Unit has been recently assigned with a new role and is being initialized
- Resync - Slave Unit is not in consistent state. This is a faulty state and should be fixed automatically during a few minutes. If this state persists, please contact support@flowmon.com

In **Action column**, there is a button **Edit unit**.


Edit unit

HWID 421E7DE5-89D6-A17E-BA3E-83

Update HWID ☐

Name Slave 1 of Proxy 1

IP address 192.168.50.105

Slave Unit Configuration Form

This button opens Slave Unit configuration form. In this form, following items are present:

- **Update HWID** - Each unit in DA is uniquely defined by its HWID. In an unlikely event of unit failure resulting to its complete replacement, the unit HWID in DA topology must be replaced as well. In this case it is necessary to check this option and click on SAVE button. Then new HWID is detected and unit is fully initialized with the original unit's configuration.
- **Name** - User defined name of the unit. Can be set to any value.
- **IP address** - IP address of the unit. For Master Unit, this IP must be reachable by users and all Master Units. For Proxy Unit, this IP must be reachable by all Master Units. For Slave Unit, this IP must be reachable by Proxy Unit from the same Proxy Group. For Unassigned Unit, the IP address must be reachable by Master Units.

Next button in the **Action column** opens Remote Configuration Center (RCC) which purpose is to configure the particular Slave Unit. In its RCC, Local configuration can be changed. Global and Source group configuration settings can be viewed but cannot be changed.

The last button in the **Action column** removes the Slave Unit from the Proxy Group.

The add new source group button

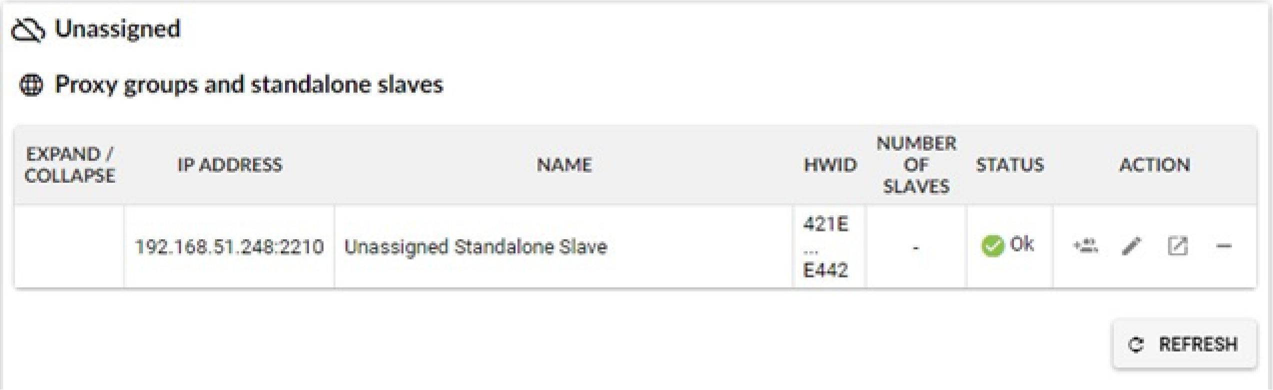
This button opens new form for adding new Source Group. In this form, name of the Source Group and Proxy mode must be defined. **Proxy mode** can be set to **Round-robin** or **Flow-source related**. If **Flow-source related mode** is selected, then as soon as flow sources are detected in the Source Group it is necessary to assign every flow source to a specific Slave Unit using Source Group Edit button (multiple flow sources can be assigned to the same Slave Unit). The flows from the particular flow source will be exported to selected Slave Unit. For **Round-robin mode**, flows from all flow sources are distributed to all **Slave Units** equally.

DA Topology Configuration - Unassigned Units

Here there are two tables listing **unassigned Proxy groups and standalone slaves** and **Units with no role**.

Proxy groups and standalone slaves

In table Proxy groups and standalone slaves, there are all Proxy Groups and Standalone Slaves which are not assigned to any Source Group.



Unassigned

Proxy groups and standalone slaves

EXPAND / COLLAPSE	IP ADDRESS	NAME	HWID	NUMBER OF SLAVES	STATUS	ACTION
	192.168.51.248:2210	Unassigned Standalone Slave	421E ... E442	-	✓ Ok	

REFRESH

Unassigned Proxy groups and standalone slaves

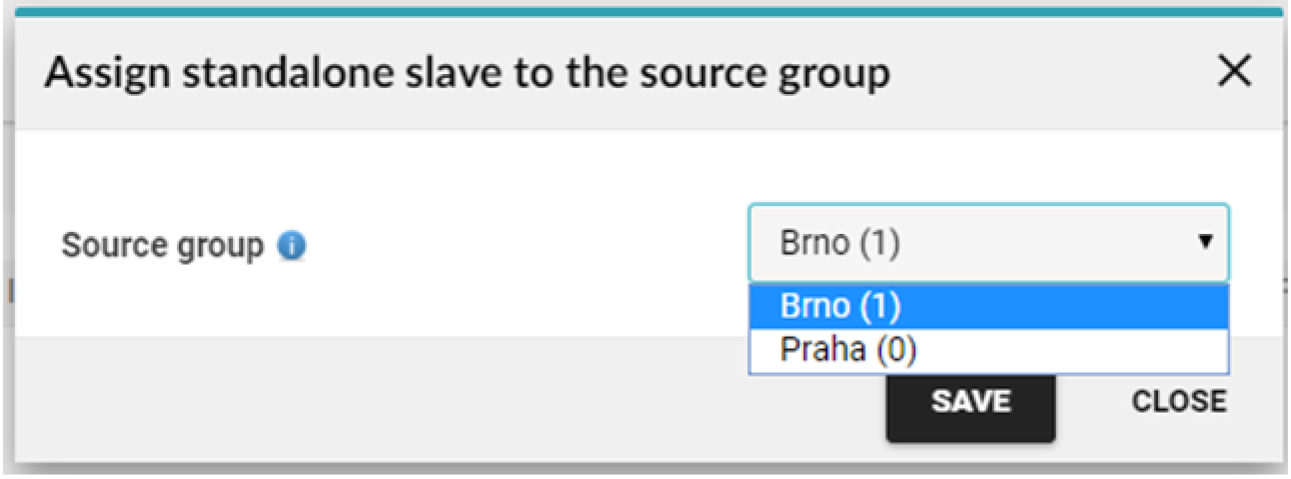
In this table, there is a **HWID column**, where the HWID of the unit is displayed. To show the full HWID, the mouse has to be hovered over the HWID shortly.

Next, there is a **Number of Slaves column**, where the number of Slave Units in Proxy Group is displayed. For Standalone Slave, there is no number displayed.

In **Status column**, the current status is displayed. The status can be set as follows>

- OK - Unit is working properly
- Init - Unit has been recently assigned with a new role and is being initialized
- Resync - Unit is not in consistent state. This is a faulty state and should be fixed automatically during a few minutes. If this state persists, please contact support@flowmon.com

In the **Action column**, there is a button **Assign to the source group**. This button opens a new form. In this form, the Source Group is selected and confirmed by **SAVE** button.

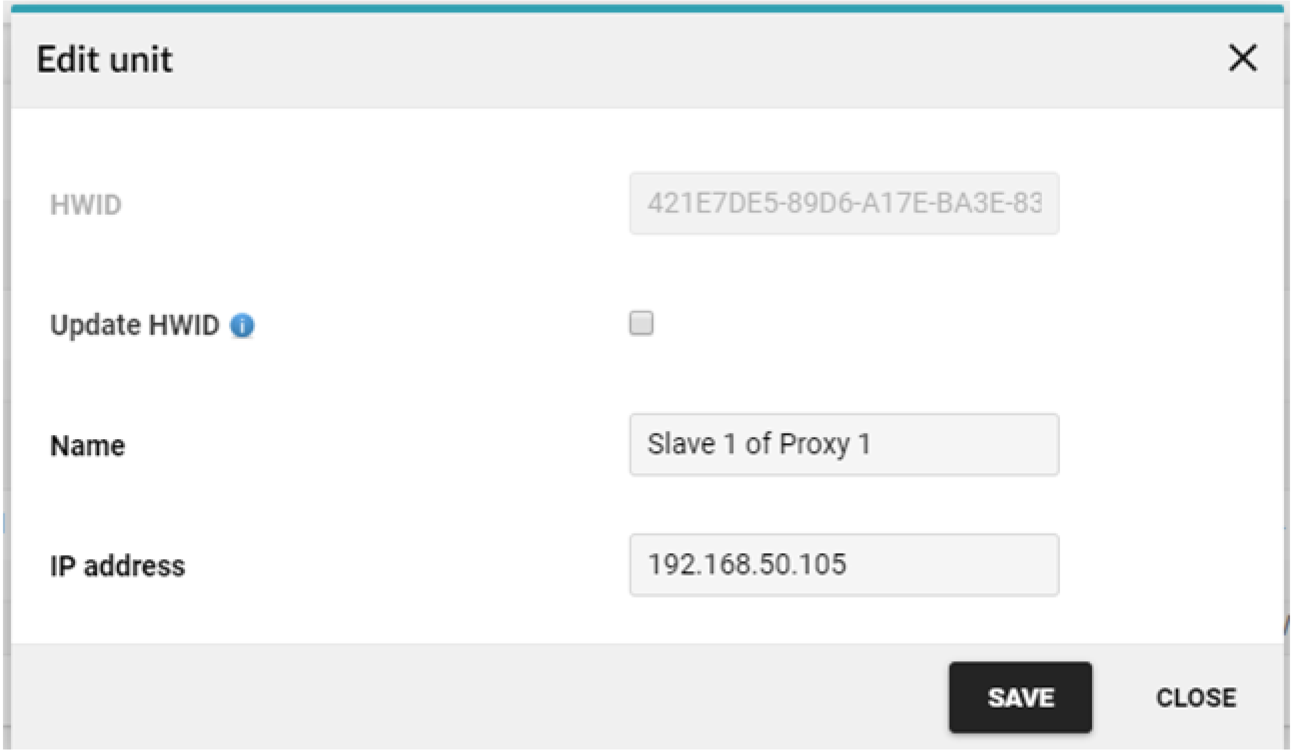


Assign standalone slave to the source group

Source group: Brno (1)

Assign Standalone Slave Into Source Group Form

Next button in the **Action column**, there is a button **Edit unit**. This button opens Proxy Unit or Standalone Slave Unit configuration form.



Edit unit

HWID	421E7DE5-89D6-A17E-BA3E-83
Update HWID	□
Name	Slave 1 of Proxy 1
IP address	192.168.50.105

Standalone Slave Unit Configuration Form

In this form, following items are present:

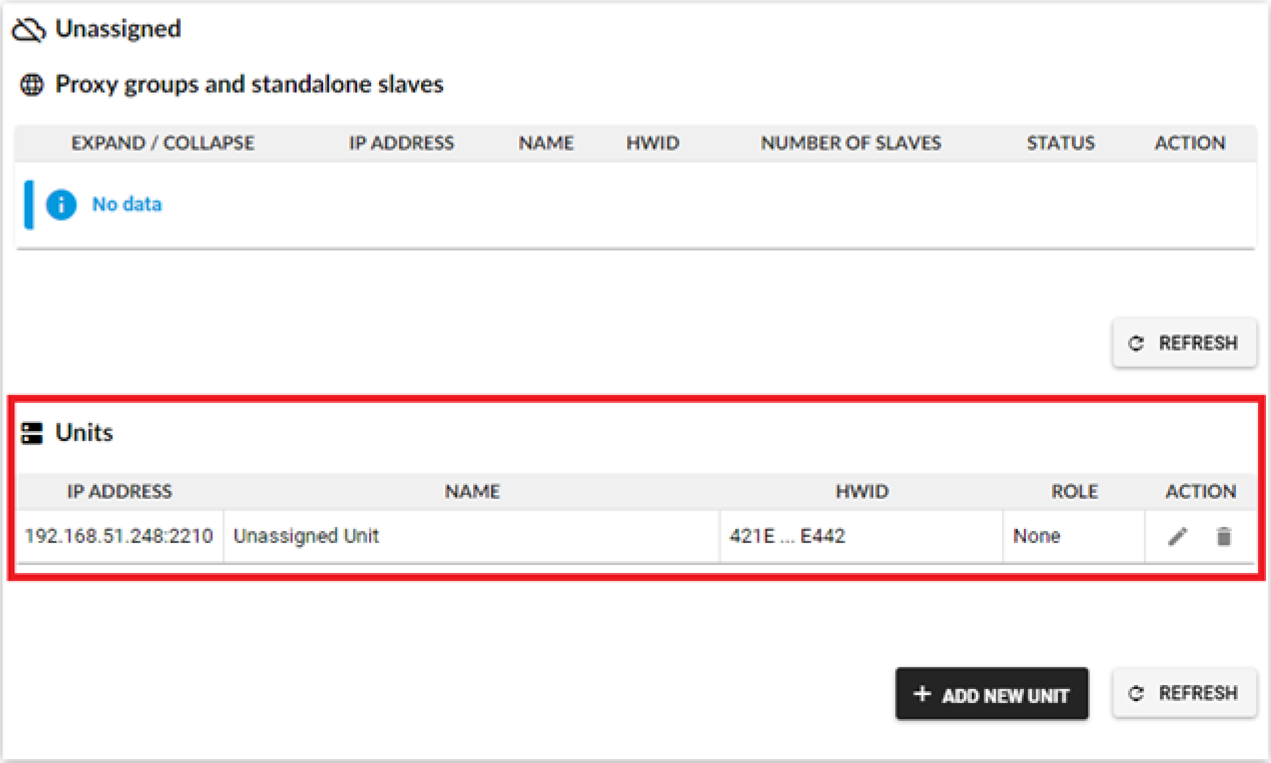
- **Update HWID** - Each unit in DA is uniquely defined by its HWID. In an unlikely event of unit failure resulting to its complete replacement, the unit HWID in DA topology must be replaced as well. In this case it is necessary to check this option and click on SAVE button. Then new HWID is detected and unit is fully initialized with the original unit's configuration.
- **Name** - User defined name of the unit. Can be set to any value.
- **IP address** - IP address of the unit. For Master Unit, this IP must be reachable by users and all Master Units. For Proxy Unit, this IP must be reachable by all Master Units. For Slave Unit, this IP must be reachable by Proxy Unit from the same Proxy Group. For Unassigned Unit, the IP address must be reachable by Master Units.

Next button in the **Action column** opens Remote Configuration Center (RCC) which purpose is to configure the particular Unit. In its RCC, Local configuration can be changed. Global configuration settings can be viewed but cannot be changed.

The last button in the **Action column** removes the role assignment from the unit so it turns the Unit into Unassigned Unit.

Units

In table Units, there are all units registered on TPM which are not assigned with any role (i.e. they are neither Master, Proxy nor Slave Unit).


Unassigned

Proxy groups and standalone slaves

EXPAND / COLLAPSE	IP ADDRESS	NAME	HWID	NUMBER OF SLAVES	STATUS	ACTION
No data						

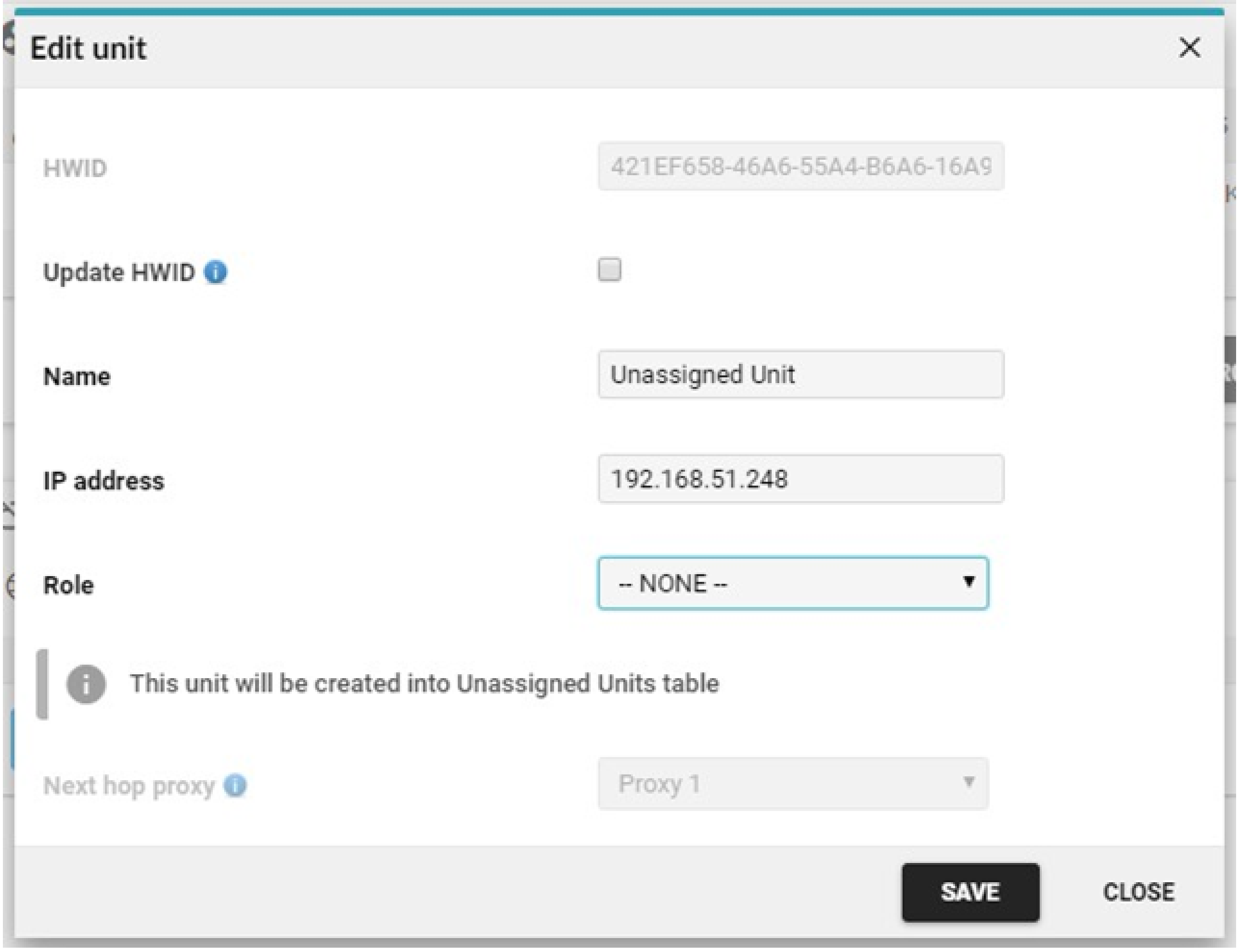
Units

IP ADDRESS	NAME	HWID	ROLE	ACTION
192.168.51.248:2210	Unassigned Unit	421E ... E442	None	

Unassigned Units

In this table, there is a **HWID column**, where the HWID of the unit is displayed. To show the full HWID, the mouse has to be hovered over the HWID shortly.

Next button in the **Action column**, there is a button **Edit unit**. This button opens Unit configuration form.


Edit unit

HWID	421EF658-46A6-55A4-B6A6-16A9
Update HWID	☐
Name	Unassigned Unit
IP address	192.168.51.248
Role	-- NONE --

This unit will be created into Unassigned Units table

Next hop proxy	Proxy 1

Unassigned Unit Configuration Form

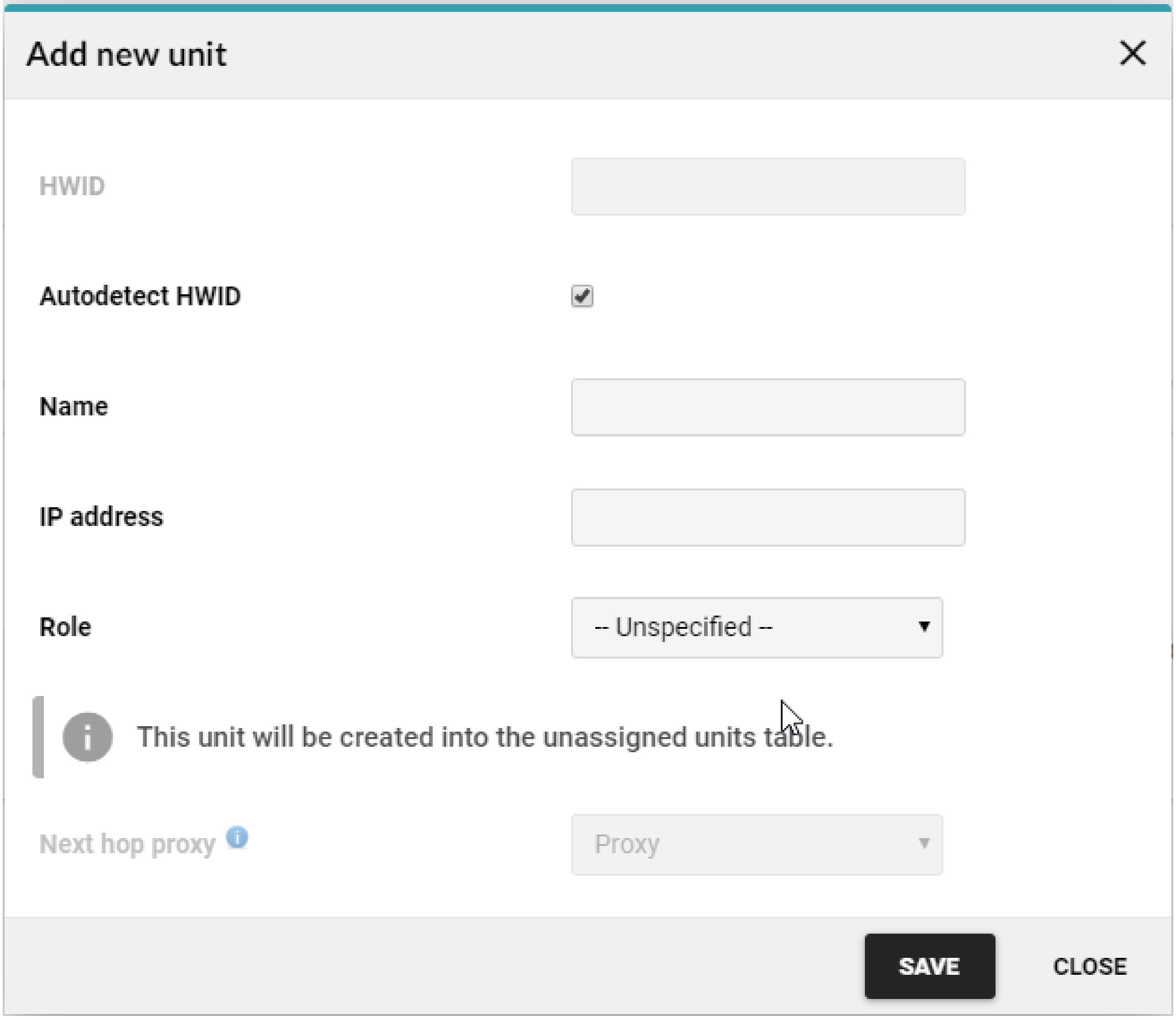
In this form, following items are present:

- **Update HWID** - Each unit in DA is uniquely defined by its HWID. In an unlikely event of unit failure resulting to its complete replacement, the unit HWID in DA topology must be replaced as well. In this case it is necessary to check this option and click on SAVE button. Then new HWID is detected and unit is fully initialized with the original unit's configuration.
- **Name** - User defined name of the unit. Can be set to any value.
- **IP address** - IP address of the unit. For Master Unit, this IP must be reachable by users and all Master Units. For Proxy Unit, this IP must be reachable by all Master Units. For Slave Unit, this IP must be reachable by Proxy Unit from the same Proxy Group. For Unassigned Unit, the IP address must be reachable by Master Units.
- **Role** - A new role can be assigned to the unit

The last button in the **Action column** deletes the unit from DA completely.

The Add new unit button

This button opens **New unit form**.



Add new unit

HWID	
Autodetect HWID	☑
Name	
IP address	
Role	-- Unspecified --

This unit will be created into the unassigned units table.

Next hop proxy	Proxy

In this form, following items are present:

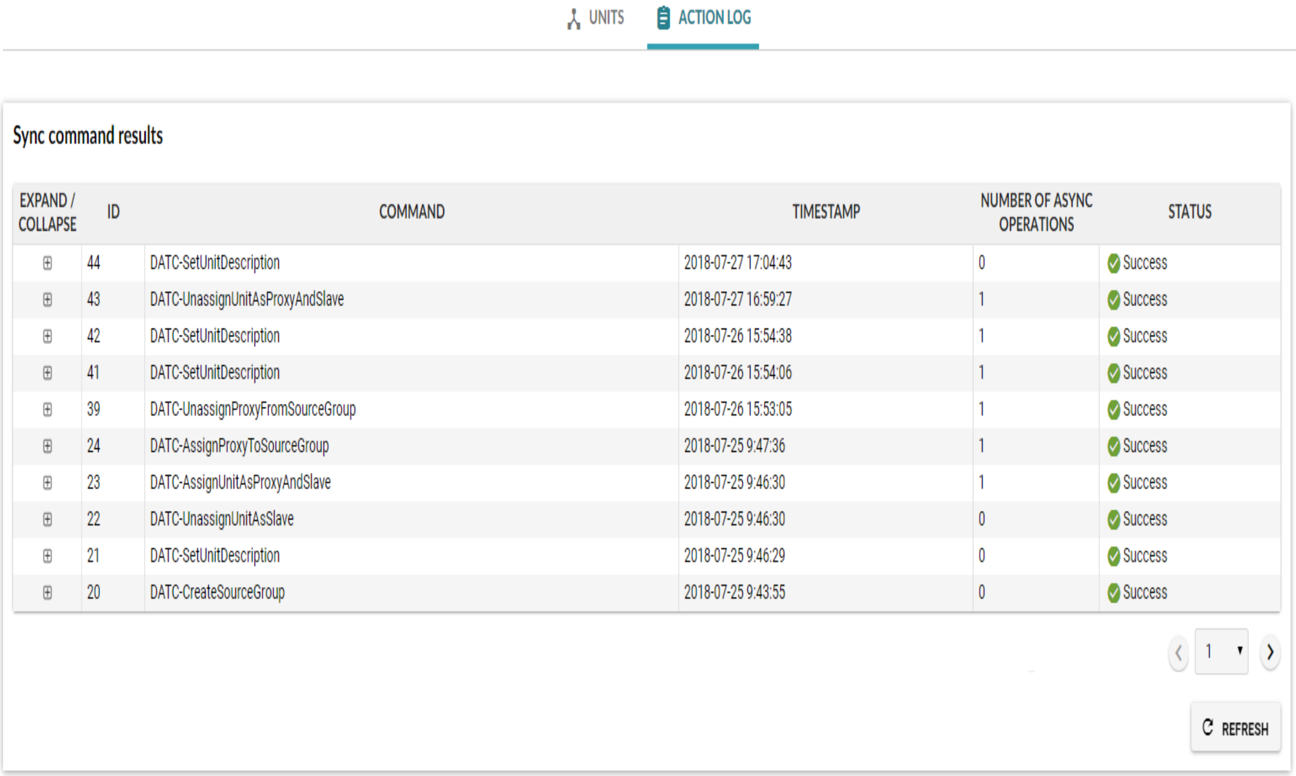
- **Autodetect HWID** - Each unit in DA is uniquely defined by its HWID. For new unit, it can be either provided by user or autodetected from the new unit. In case of autodetection, the unit must be reachable from TPM unit or via next hop Proxy (in case the new unit is configured as a Slave Unit).

- **Name** - User defined name of the unit. Can be set to any value.
- **IP address** - IP address of the unit. For Master Unit, this IP must be reachable by users and all Master Units. For Proxy Unit, this IP must be reachable by all Master Units. For Slave Unit, this IP must be reachable by Proxy Unit from the same Proxy Group. For Unassigned Unit, the IP address must be reachable by Master Units.
- **Role** - A new role can be assigned to the unit

Action Log

In tab **Action Log** all topology operations can be reviewed and their result can be checked.

Operations on remote units can be performed asynchronously. Their result can be checked in this log when the particular event is expanded by expand button.



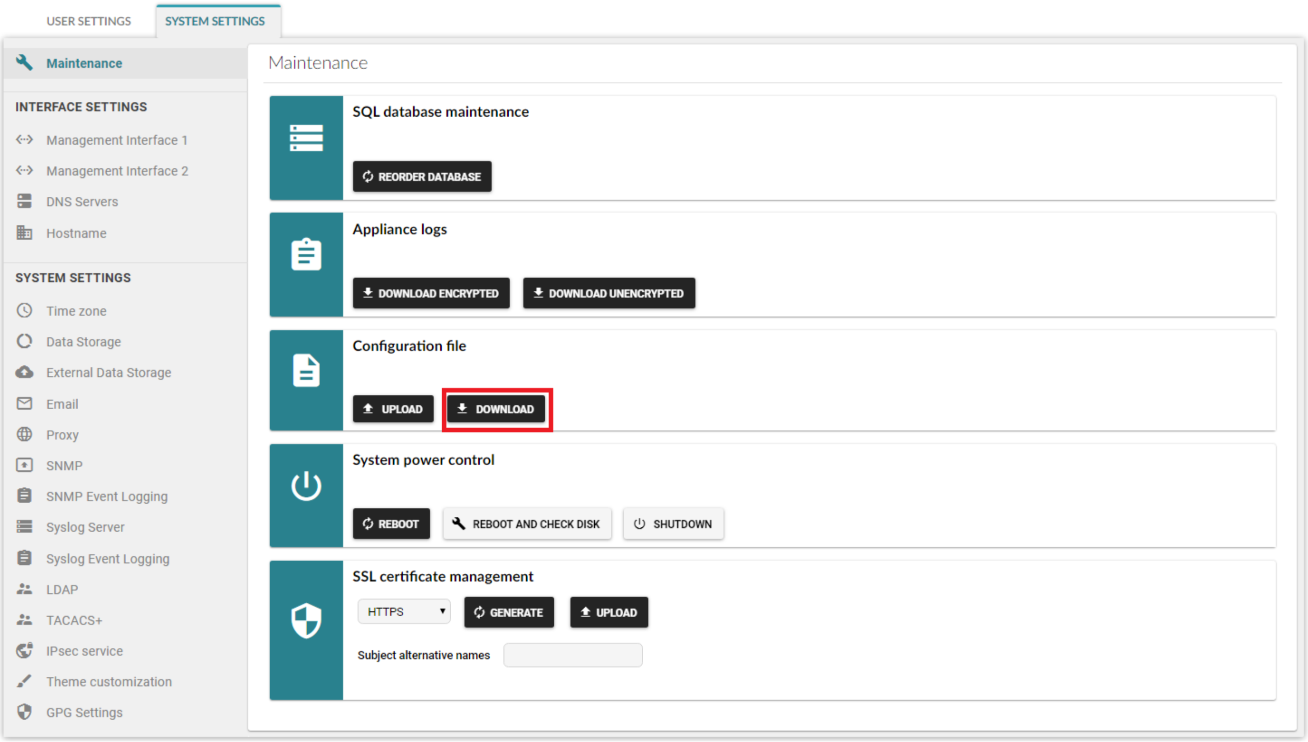
Sync command results

EXPAND / COLLAPSE	ID	COMMAND	TIMESTAMP	NUMBER OF ASYNC OPERATIONS	STATUS
⊞	44	DATC-SetUnitDescription	2018-07-27 17:04:43	0	✓ Success
⊞	43	DATC-UnassignUnitAsProxyAndSlave	2018-07-27 16:59:27	1	✓ Success
⊞	42	DATC-SetUnitDescription	2018-07-26 15:54:38	1	✓ Success
⊞	41	DATC-SetUnitDescription	2018-07-26 15:54:06	1	✓ Success
⊞	39	DATC-UnassignProxyFromSourceGroup	2018-07-26 15:53:05	1	✓ Success
⊞	24	DATC-AssignProxyToSourceGroup	2018-07-25 9:47:36	1	✓ Success
⊞	23	DATC-AssignUnitAsProxyAndSlave	2018-07-25 9:46:30	1	✓ Success
⊞	22	DATC-UnassignUnitAsSlave	2018-07-25 9:46:30	0	✓ Success
⊞	21	DATC-SetUnitDescription	2018-07-25 9:46:29	0	✓ Success
⊞	20	DATC-CreateSourceGroup	2018-07-25 9:43:55	0	✓ Success

The Action log table

How To Backup Configuration of DA Units and Source Groups

Configuration of DA Units and Source Groups can be downloaded in Remote Configuration Center of particular unit or Source Group. Configuration of TPM Unit and whole DA topology can be downloaded on TPM in its local FCC. The download in all cases is performed in System page, Maintenance tab, Configuration file section, Download button.



Configuration backup

How to change DA unit’s IP address

If a DA unit’s IP address has been changed, you need to change it also on TPM in Distributed Architecture page.

Replacing Faulty DA Units

In case some of the units connected into DA fails and needs to be reset to factory default setting or replaced by a new unit, it can be done by the process described in the following chapters.

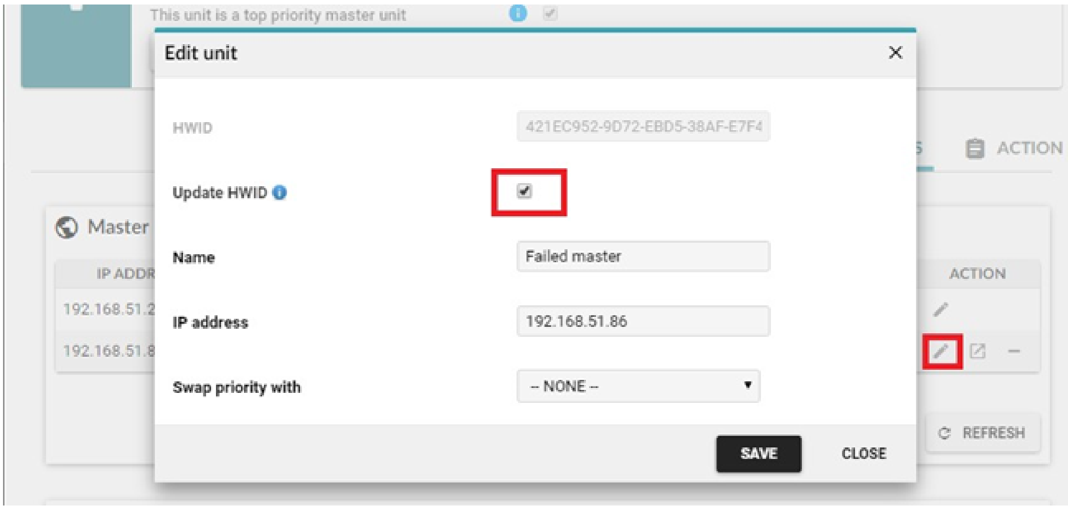
If you have installed Flowmon ADS module in distributed configuration, please check this chapter for details about ADS recovery process.

How to replace faulty TPM unit When Backup Master Units are Present

This chapter describes how to replace faulty TPM unit in case multiple Master Units are connected into DA.

- On the Master Unit with lower priority, open Flowmon Configuration Center, Distributed Architecture and select option This unit is top priority master unit.
- The lower priority Master Unit is turned into TPM.
- Replace failed Master unit with a new unit. Select the same IP address on its management interface and enable Distributed Architecture.
- On new TPM, in Distributed Architecture page, in Master Units table, edit the failed Master Unit, select Update HWID option and click the SAVE button. See the picture below.
- Replaced Master Unit will be added into DA with new HWID and the original Master Unit configuration will be applied to the new Unit.

- When new Master Unit status is OK, you can swap the priority back to the original Master (optional).



Edit unit

HWID	421EC952-9D72-EBD5-38AF-E7F4
Update HWID	☑
Name	Failed master
IP address	192.168.51.86
Swap priority with	-- NONE --

How to Faulty TPM Unit When No Backup Master Units are Present

This chapter describes how to replace faulty TPM in case there are no other Master Units connected into DA. To make this possible, it is necessary to backup your TPM and DA configuration after every change! The guide on how to make it can be found in this section.

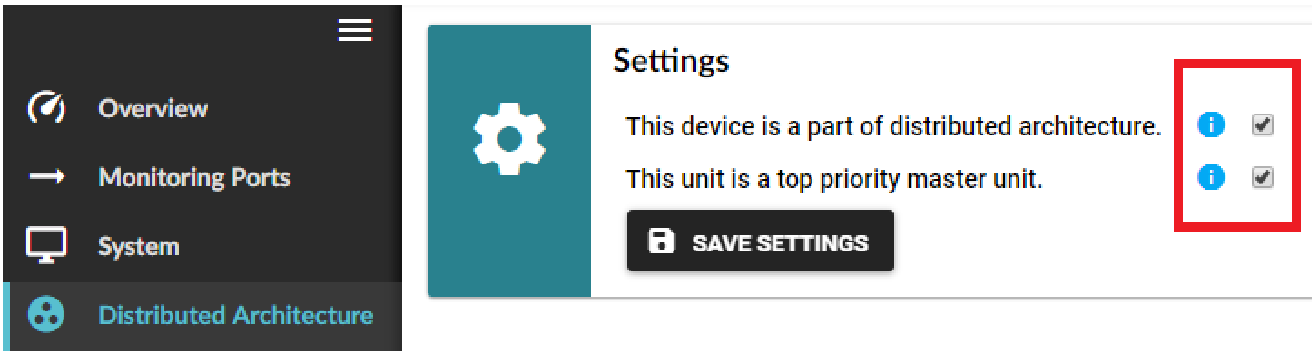
If you have a backup ready, you can replace the faulty TPM by the following steps.

- Replace/fix the faulty TPM unit. **Important:** Make sure that Flowmon OS and all modules are installed in the same versions as on the failed TPM.

- Check, whether the Flowmon license is still valid. It might become invalid if some part of hardware has been replaced. Request new license if necessary and upload it to the device.
- Login to the command line (CLI interface) and run the following command. It will restore the unit into the factory settings:

```
./restore_factory_settings.sh autorun
```

- On replaced TPM, configure the same IP address.
- Enable DA and TPM mode.

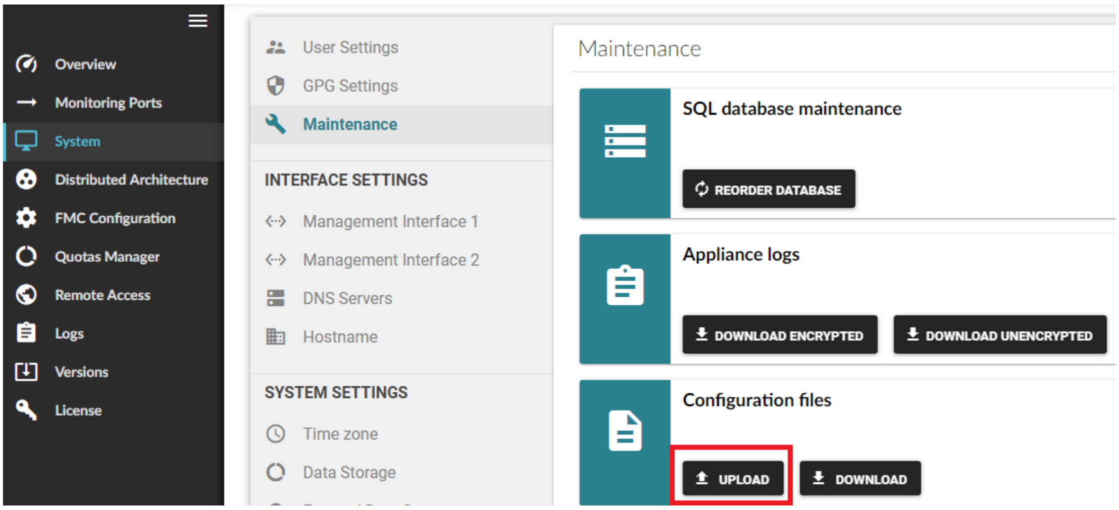


Settings

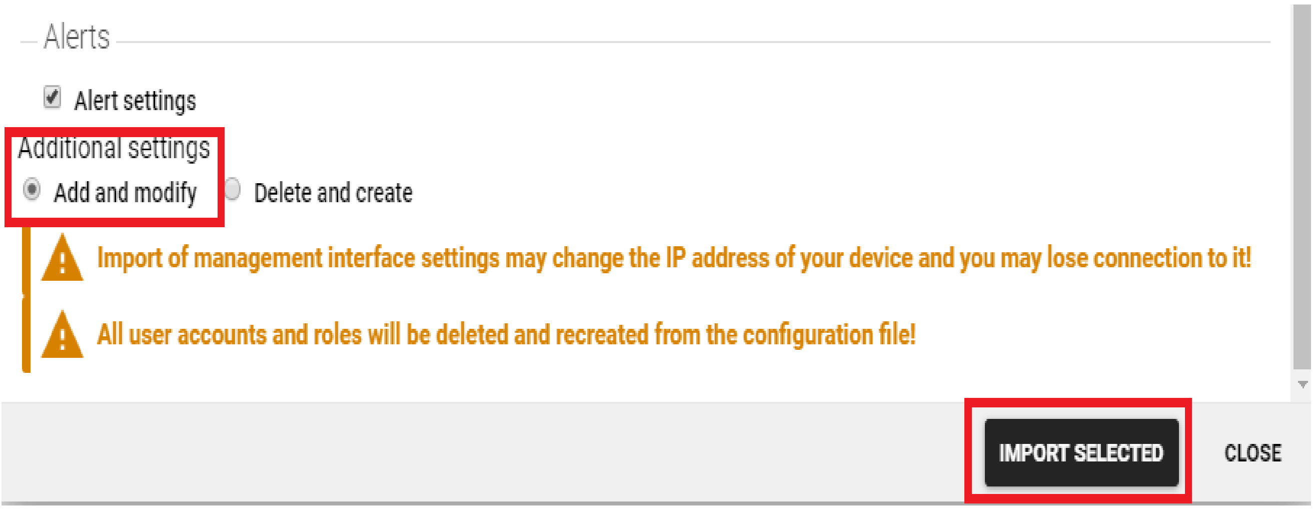
This device is a part of distributed architecture. ☑

This unit is a top priority master unit. ☑

- Upload the backup configuration.



- Select all sections for import (including Distributed Architecture). Choose Add and modify mode. Then click IMPORT SELECTED.



Alerts

☑ Alert settings

Additional settings

● Add and modify ○ Delete and create

Import of management interface settings may change the IP address of your device and you may lose connection to it!

All user accounts and roles will be deleted and recreated from the configuration file!

- Now the TPM unit is recovered.

Important: No data are lost on proxy or slave units however the profile graphs are not recovered. They start to be computed once the new TPM is configured. However, as the flow data are available, users can still make a query and reports over older data with no graph. Also the Reports data have to be recomputed manually for the history.

How to Replace Faulty Unit

This chapter describes how to replace any other DA unit but TPM (e.g. Slave Unit etc.). Failed unit can be replaced as follows:

- Replace/fix the failed unit with a new unit.

- Check, whether the Flowmon license is still valid. It might become invalid if some part of hardware has been replaced. Request a new license if necessary and upload it to the device.
- Login to the command line (CLI interface) and run the following command. It will restore the unit into the factory settings:

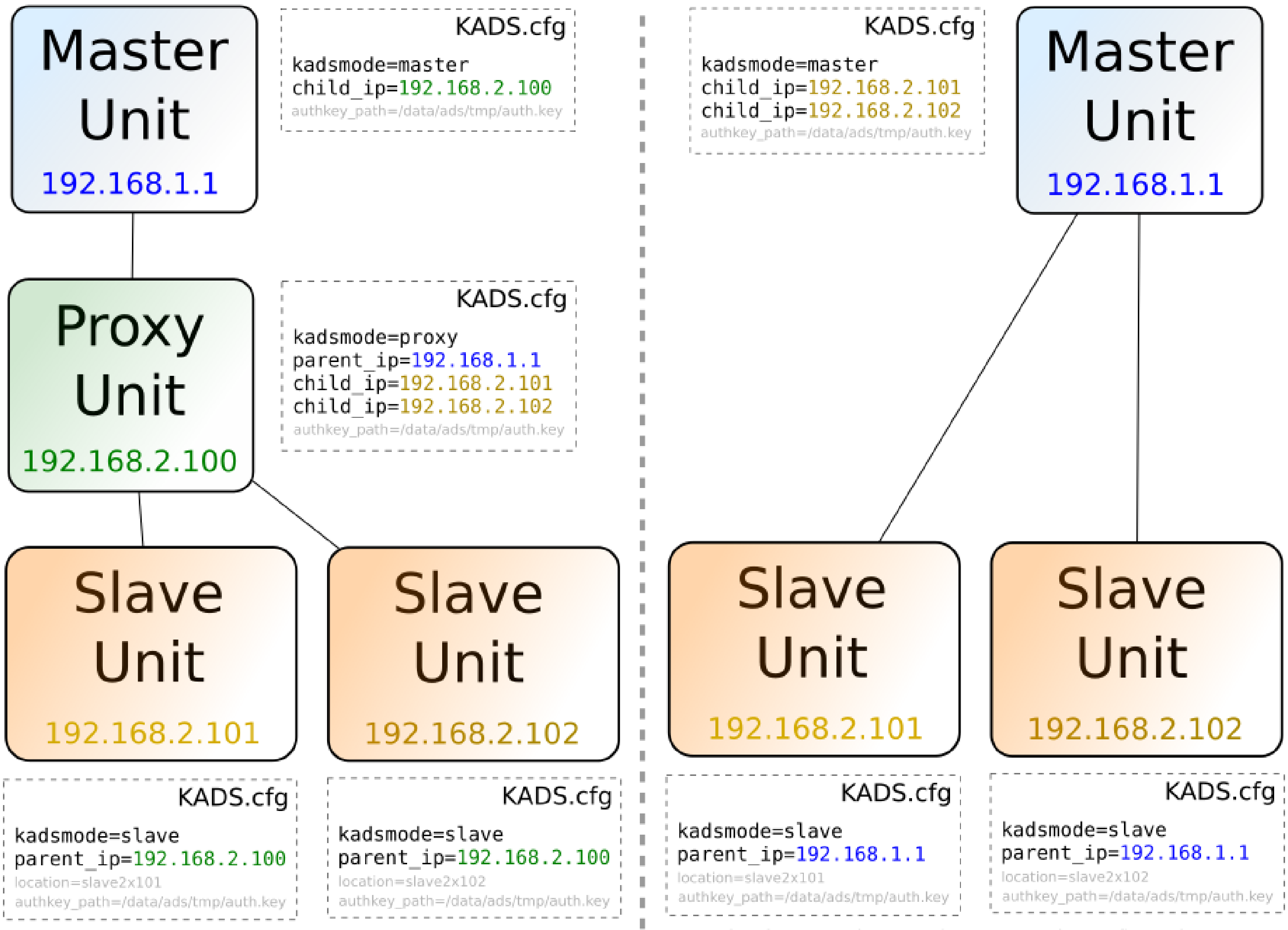
```
./restore_factory_settings.sh autorun
```

- Select the same IP address on its management interface and enable Distributed Architecture.
- On TPM, in Distributed Architecture page, in Master Units table, edit the failed Unit, select Update HWID option and click the SAVE button.
- Replaced Unit will be added into DA with new HWID and the configuration of the original Unit will be applied to the new Unit.

How to Recover Distributed ADS on Replaced Unit

ADS configuration and events are stored on Master Unit only. Distributed ADS does not support more than one Master Unit (backup). **We recommend to backup ADS configuration after every change manually** via Flowmon Configuration Center. There is no simple way to backup/restore the whole database of detected events. We recommend to send the event to a third party system via syslog event reporting to archive. Flowmon ADS Distributed architecture is configured independently on Flowmon Distributed Architecture and need to be fixed manually.

Configuration of Flowmon ADS Distributed Architecture is stored in configuration file */data/ads/KADS.cfg* on each unit. The file contains information about mode of unit (master, slave, proxy) and IP addresses of related units from the unit point of view. KADS.cfg can be managed manually or via ADS DA configuration wizard (recommended). See ADS user guide for more information.



KADS.cfg

```
kadsmode=master
child_ip=192.168.2.100
authkey_path=/data/ads/tmp/auth.key
```

KADS.cfg

```
kadsmode=proxy
parent_ip=192.168.1.1
child_ip=192.168.2.101
child_ip=192.168.2.102
authkey_path=/data/ads/tmp/auth.key
```

KADS.cfg

```
kadsmode=slave
parent_ip=192.168.2.100
location=slave2x101
authkey_path=/data/ads/tmp/auth.key
```

KADS.cfg

```
kadsmode=slave
parent_ip=192.168.2.100
location=slave2x102
authkey_path=/data/ads/tmp/auth.key
```

KADS.cfg

```
kadsmode=master
child_ip=192.168.2.101
child_ip=192.168.2.102
authkey_path=/data/ads/tmp/auth.key
```

KADS.cfg

```
kadsmode=slave
parent_ip=192.168.1.1
location=slave2x101
authkey_path=/data/ads/tmp/auth.key
```

KADS.cfg

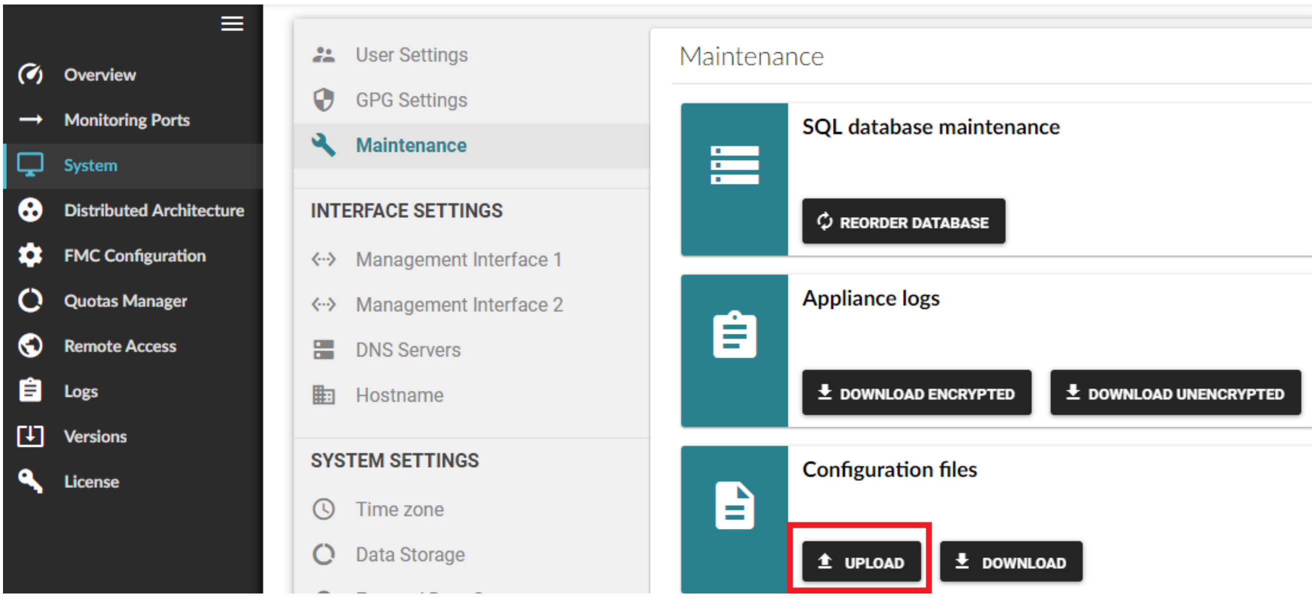
```
kadsmode=slave
parent_ip=192.168.1.1
location=slave2x102
authkey_path=/data/ads/tmp/auth.key
```

Example of Master-Proxy-Slave Deployment Mode Configuration

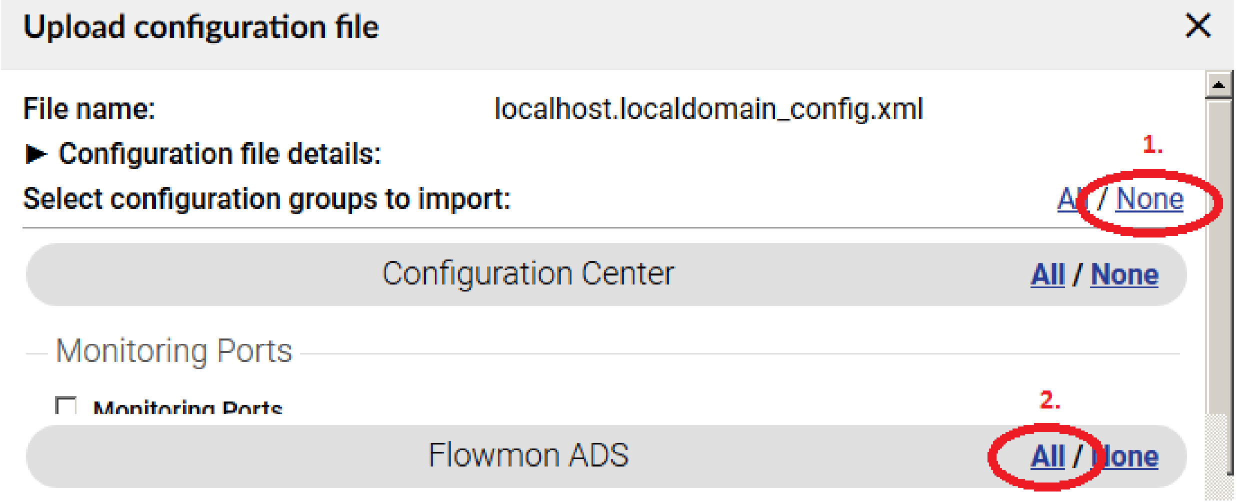
Example of Master-Slave Deployment Mode Configuration

Replacing Master Unit

- Follow Flowmon OS instructions of replacing faulty TPM unit first
  - Working TPM and installed ADS are expected before continue
- Upload ADS configuration from your backup



- Select ADS configuration group
  - Unselect all configuration groups by clicking on None
  - Select ADS group only by clicking on All in ADS section



Upload configuration file
File name: localhost.localdomain_config.xml
▶ Configuration file details:
Select configuration groups to import:
1.
All / None
Configuration Center
All / None
Monitoring Ports
□ Monitoring Ports
2.
Flowmon ADS
All / None

- Clean previous Flowmon ADS Distributed Architecture configuration (optional)
  - This step **can be skipped when ADS DA was configured via kads wizard before** (not manually) **and only Master Unit is replaced** (all other units will be reconfigured during new initialization).
  - Login to each unit as user flowmon via SSH protocol and perform following steps:
    - Open configuration file /data/ads/KADS.cfg
      - Comment out lines starting with keywords:
        - kadsmode, child_ip, parent_ip, authkey_path
    - Remove ADS DA SSH auth public key
      - Open /home/flowmon/.ssh/authorized_keys
      - Remove line with ADS DA auth key
    - Remove ADS DA SSH auth private key
      - Remove files /data/ads/tmp/auth.key*
    - Restart Flowmon ADS module
      - sudo /etc/flowmon/plugins/flowmon-ads/start_stop.sh stop
      - sudo /etc/flowmon/plugins/flowmon-ads/start_stop.sh start

- Initialize Flowmon ADS Distributed Architecture

Log to Flowmon OS terminal on Master unit and execute **kads-wizard.py** command to start Flowmon ADS DA configuration wizard.

```
ADS Wizard initialization…
...checking local configuration files.
...reading local configuration.
! No 'kadsmode' configuration found.

Do you want to start master configuration? (yes/no):
```

- Type yes and press enter to initialize ADS DA

After successful initialization, add all Slave/Proxy units via *Assign New unit to Master* menu option

```
Welcome to KADS Configuration Wizard.

Master: 192.168.1.1 (NO CHILDS DEFINED)

What do you want to do?
     1) Assign new Unit to Master
     2) Deinitialize Distributed Architecture
     3) Show status
     4) Exit

Select number:
```

- *See Distributed Architecture Quickstart Guide* or ADS user guide for more information

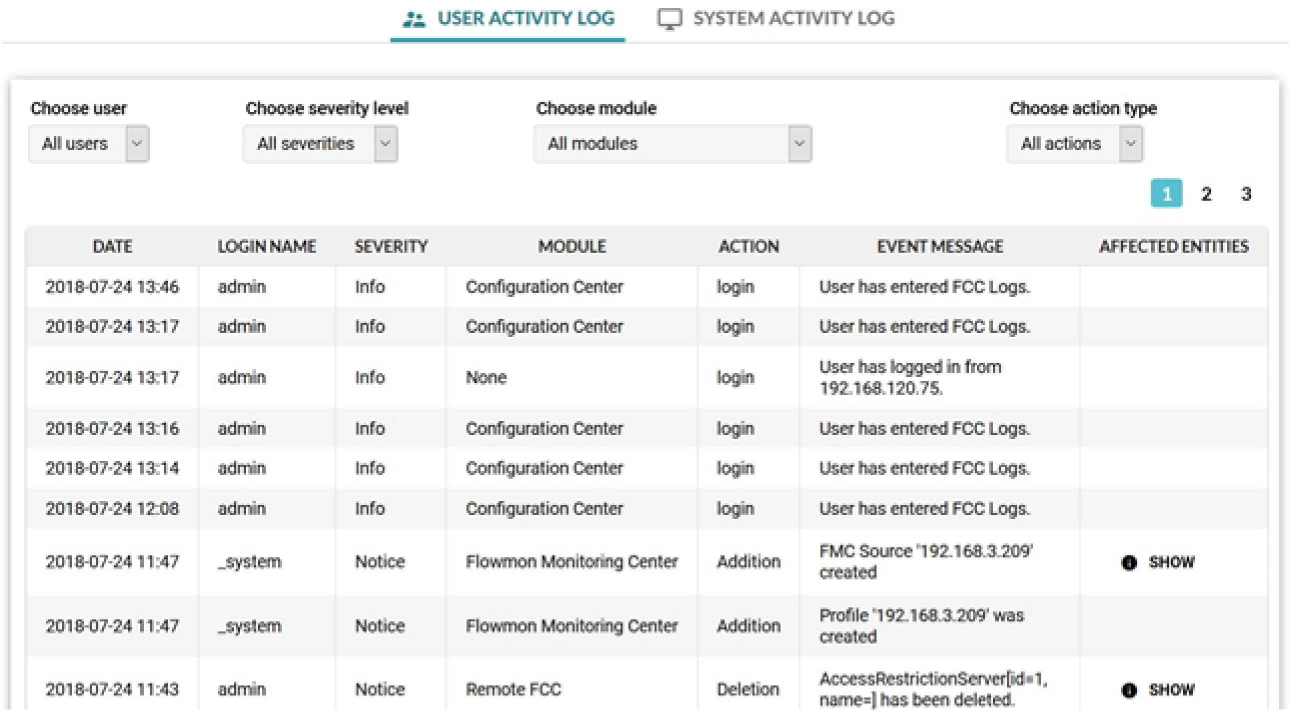
- Check Flowmon ADS quotas on Master Unit
    - FCC - Quota Manager (used for storing events, 10 GB at least)
    - FCC - Distributed Architecture - Source Group - Open FCC - Quota Manager (used for backend processing on Slaves, set to 50 GB for each Source Group)

Replacing Proxy/Slave Unit

- Remove replaced unit from related units
    - Login to **each** related unit as user flowmon via SSH protocol
    - Open configuration file /data/ads/KADS.cfg
        - Remove line with IP of replaced unit
- Clean replaced unit (optional)
    - This step **can be skipped when unit is not available anymore** (dead, reinstalled completely) or removed (deinitialized) via kads wizard cleanly.
    - Login to replaced failed unit as user flowmon via SSH protocol
    - Open configuration file /data/ads/KADS.cfg
        - Comment out lines starting with keywords:
            - kadsmode, child_ip, parent_ip, authkey_path
    - Remove ADS DA SSH auth public key
        - Open /home/flowmon/.ssh/authorized_keys
        - Remove line with ADS DA auth key
    - Remove ADS DA SSH auth private key
        - Remove files /data/ads/tmp/auth.key*
    - Restart Flowmon ADS module
        - sudo /etc/flowmon/plugins/flowmon-ads/start_stop.sh stop
        - sudo /etc/flowmon/plugins/flowmon-ads/start_stop.sh start
- Add new unit
    - Login to Master unit as user flowmon via SSH protocol
    - Open /home/flowmon/.ssh/known_hosts and remove line with old Slave identity
    - Run kads-wizard.py
    - Assign new Unit to Master/Proxy via wizard menu
- Check Flowmon ADS quotas on Master Unit
    - FCC - Quota Manager (used for storing events, 10 GB at least)
    - FCC - Distributed Architecture - Source Group - Open FCC - Quota Manager (used for backend processing on Slaves, set to 50 GB for each Source Group)

Logs

This page show two different types of logs, available in two tabs. The **User Activity Log** tab included all actions (especially changes) performed in the system. This list can be filter by users, modules and actions (add, change, delete etc.). You can also select specific severity level, this choice will show only the events with the given severity level or the higher. System logs are located in the **System Activity Log** tab.



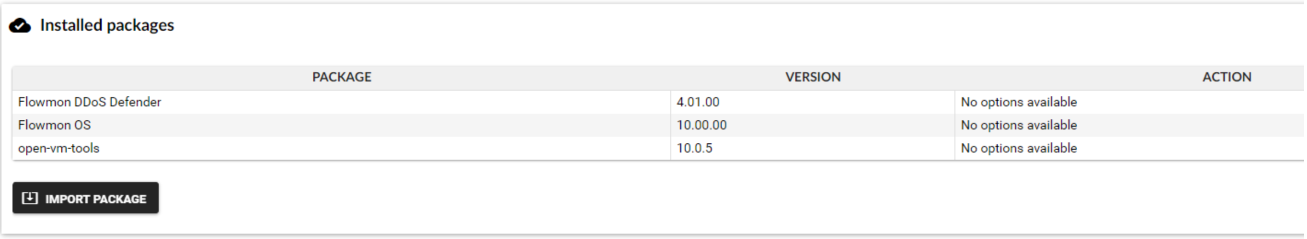
Choose user: All users
Choose severity level: All severities
Choose module: All modules
Choose action type: All actions

DATE	LOGIN NAME	SEVERITY	MODULE	ACTION	EVENT MESSAGE	AFFECTED ENTITIES
2018-07-24 13:46	admin	Info	Configuration Center	login	User has entered FCC Logs.	
2018-07-24 13:17	admin	Info	Configuration Center	login	User has entered FCC Logs.	
2018-07-24 13:17	admin	Info	None	login	User has logged in from 192.168.120.75.	
2018-07-24 13:16	admin	Info	Configuration Center	login	User has entered FCC Logs.	
2018-07-24 13:14	admin	Info	Configuration Center	login	User has entered FCC Logs.	
2018-07-24 12:08	admin	Info	Configuration Center	login	User has entered FCC Logs.	
2018-07-24 11:47	_system	Notice	Flowmon Monitoring Center	Addition	FMC Source '192.168.3.209' created	SHOW
2018-07-24 11:47	_system	Notice	Flowmon Monitoring Center	Addition	Profile '192.168.3.209' was created	
2018-07-24 11:43	admin	Notice	Remote FCC	Deletion	AccessRestrictionServer[id=1, name=] has been deleted.	SHOW

System logs panel

Versions

This page is intended for installation and management of updates and extension packages (modules). In the table Installed Packages there is shown the actual Flowmon Networks device version and all installed modules including their versions and buttons for management (**Stop, Start, Uninstall**). To install a new version of Flowmon Probe software or a module, either press **Import package** button and install it or press **Install this package** button in Action column of the desired package in the Available packages.



Installed packages

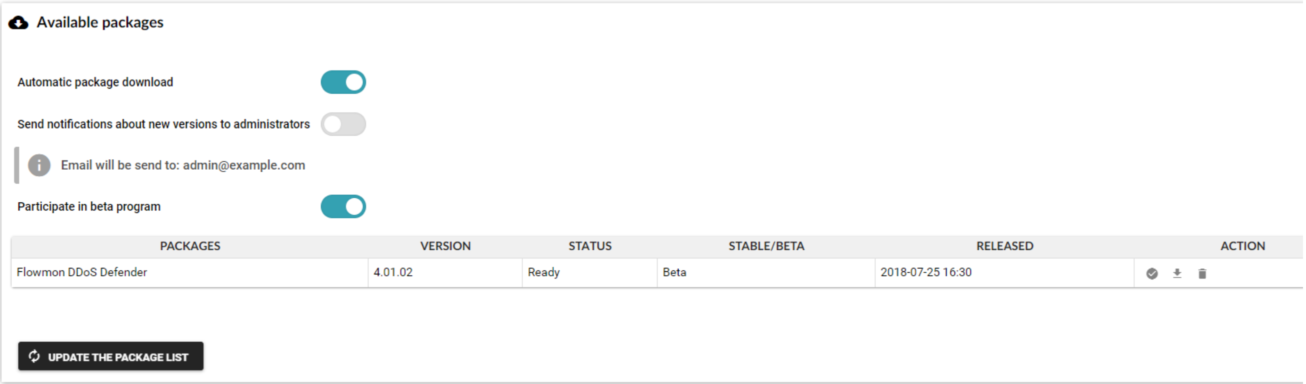
PACKAGE	VERSION	ACTION
Flowmon DDoS Defender	4.01.00	No options available
Flowmon OS	10.00.00	No options available
open-vm-tools	10.0.5	No options available

Installed packages panel

Warning

Once the install process is started, you MUST NOT reboot or turn off your device until the process is finished. When it is finished successfully, the green message will appear. In case of error, a red message will appear otherwise. Do not restart or shutdown your device during the installation process by no means and wait until it is successfully finished! Sometimes it can take even tens of minutes. If the installation is not finished by success or error message and a blank page appears in your browser, please contact support@flowmon.com.

In the table Available Packages there are available newer version of already installed packages downloaded from **services.flowmon.com** portal. Each package is downloaded only if there is a valid license for this package. System checks portal for new packages automatically every 10 minutes (if option **Automatic package download** is checked) or if the **Update package list** button is pressed. If option **Send notifications about new versions to administrators** is checked, then a notification about new version is sent to all users in group admin. If option **Participate in beta program** is checked, then also beta versions are downloaded. Beta versions offer newer functions but are not so stable.



Available packages

Automatic package download ●

Send notifications about new versions to administrators ○

Email will be send to: admin@example.com

Participate in beta program ●

PACKAGES	VERSION	STATUS	STABLE/BETA	RELEASED	ACTION
Flowmon DDoS Defender	4.01.02	Ready	Beta	2018-07-25 16:30	✓ ⭳ 🗑

Packages for installation

Once the package is downloaded, its checksum is computed. If it was downloaded correctly, it can be installed with **Install** button. If the package is installed correctly, the downloaded package will be removed during next update from portal.

Package can also be uploaded into Available Packages list manually. Upload the file via SSH into /data/packages directory and run command:

```
/usr/bin/php /var/www/shtml/index.php Cli:AddPackageManualy
-package_name=<package-name>
-major_version=<major-version>
-minor_version=<minor-version>
-build=<build-number>
-beta=<true|false>
-filename=<package-file-name>
```

- **package_name** - is the name of package without version label (i.e. flowmonplug-ads)
- **major_version**, **minor_version** and **build** - stands for number in version label, for example for package flowmonplug-ads-v6.04.01 are the number 6, 4 and 1 in the same order. In case a number is missing in package name, use 0 instead.
- **beta** - beta parameter can be of value **true** (for beta package) or **false** (for stable package)
- **filename** - is the name of file uploaded into /data/packages

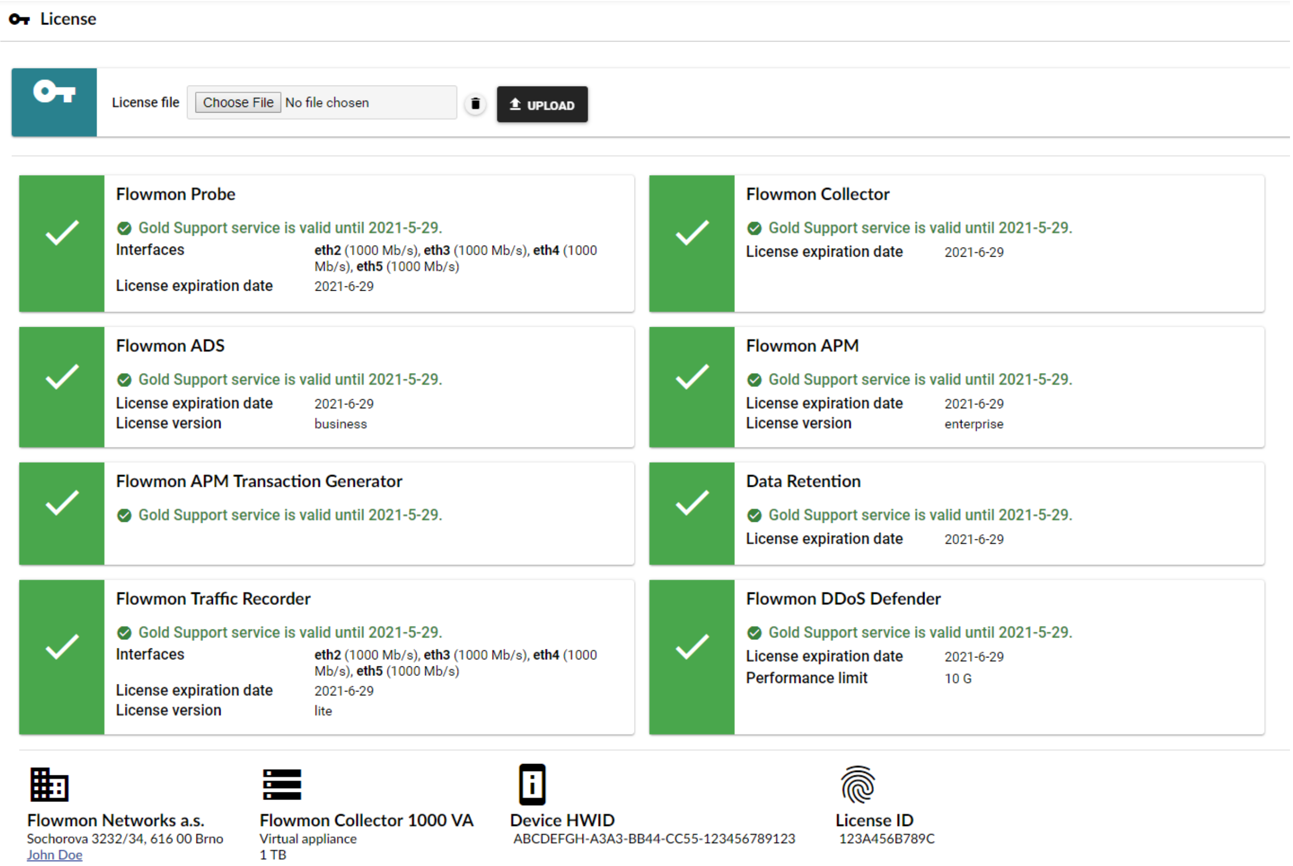
Example

```
/usr/bin/php /var/www/shtml/index.php Cli:AddPackageManualy
-package_name=flowmonplug-ads
-major_version=6 -minor_version=4
-build=1 -beta=false
-filename=flowmonplug-ads-v6.04.01.tar.gz
```

If the manual package upload is successful, it is shown in table Available packages. In this case, the package integrity is not checked (it will be done during installation) and package can be deleted only manually by clicking on **Delete** button.

License

On this page, you can check all your valid licenses and Gold and Platinum Supports and insert license file. The valid license file is already uploaded for the first power-on (not applies for virtual devices). In the case you use the Recovery CD to restore your device to the factory settings or if you somehow delete your license file, you need to choose the licence file and press **Upload** button to ensure the device will work properly. Here you can also check if the license is valid.



Flowmon Probe
Gold Support service is valid until 2021-5-29.
Interfaces: **eth2** (1000 Mb/s), **eth3** (1000 Mb/s), **eth4** (1000 Mb/s), **eth5** (1000 Mb/s)
License expiration date: 2021-6-29

Flowmon Collector
Gold Support service is valid until 2021-5-29.
License expiration date: 2021-6-29

Flowmon ADS
Gold Support service is valid until 2021-5-29.
License expiration date: 2021-6-29
License version: business

Flowmon APM
Gold Support service is valid until 2021-5-29.
License expiration date: 2021-6-29
License version: enterprise

Flowmon APM Transaction Generator
Gold Support service is valid until 2021-5-29.

Data Retention
Gold Support service is valid until 2021-5-29.
License expiration date: 2021-6-29

Flowmon Traffic Recorder
Gold Support service is valid until 2021-5-29.
Interfaces: **eth2** (1000 Mb/s), **eth3** (1000 Mb/s), **eth4** (1000 Mb/s), **eth5** (1000 Mb/s)
License expiration date: 2021-6-29
License version: lite

Flowmon DDoS Defender
Gold Support service is valid until 2021-5-29.
License expiration date: 2021-6-29
Performance limit: 10 G

Flowmon Networks a.s.
Sochorova 3232/34, 616 00 Brno
John Doe

Flowmon Collector 1000 VA
Virtual appliance
1 TB

Device HWID
ABCDEFGH-A3A3-BB44-CC55-123456789123

License ID
123A456B789C

License Page

It’s also possible to upload additional sublicenses (marked "Sublicense") with individual expiration dates.

Additional license information (company, address and person), device model and Device HWID are shown at the bottom of the page.

Flowmon Monitoring Center

The following sections describe the usage of the Flowmon Monitoring Center (FMC). FMC is controlled via web interface which provides user-friendly and intuitive control over the major functions.

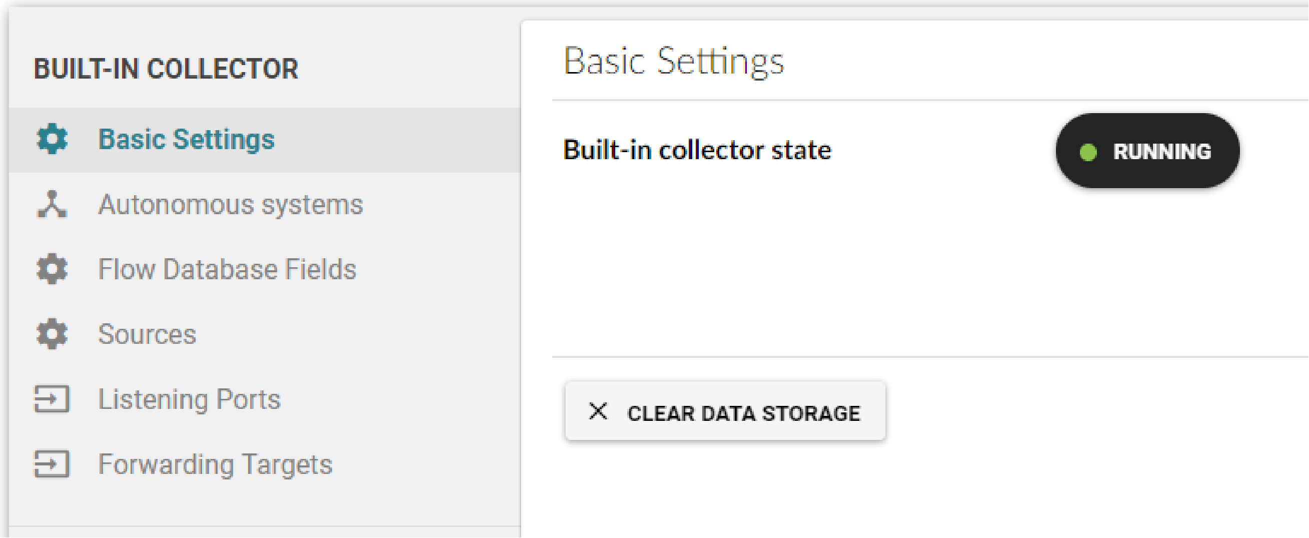
FMC Configuration

This page contains Flowmon Monitoring Center (FMC) settings and is further divided into 3 sections, each for particular part of FMC.

Built-In Collector

Built-in collector can be set up on the **FMC Configuration - Built-In Collector** page.

Use this page to perform configuration changes to built-in collector. Press **Start/Stop** button to start/stop built-in collector. You can see collector status on this button (Running/Stopped). You will not be able to access the Flowmon Monitoring Center if built-in collector is stopped.



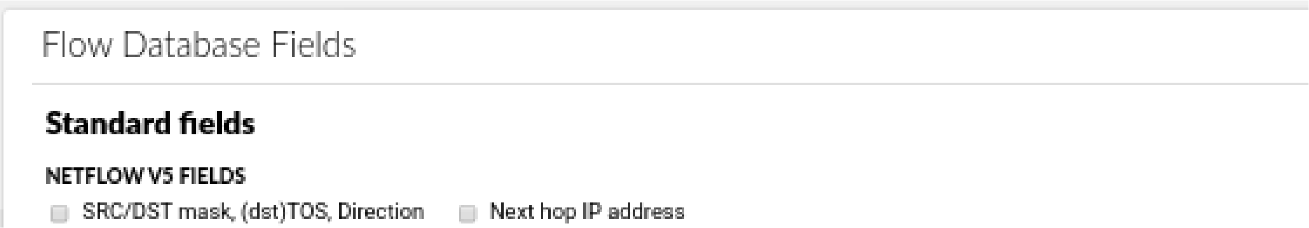
The Built-in Collector Settings

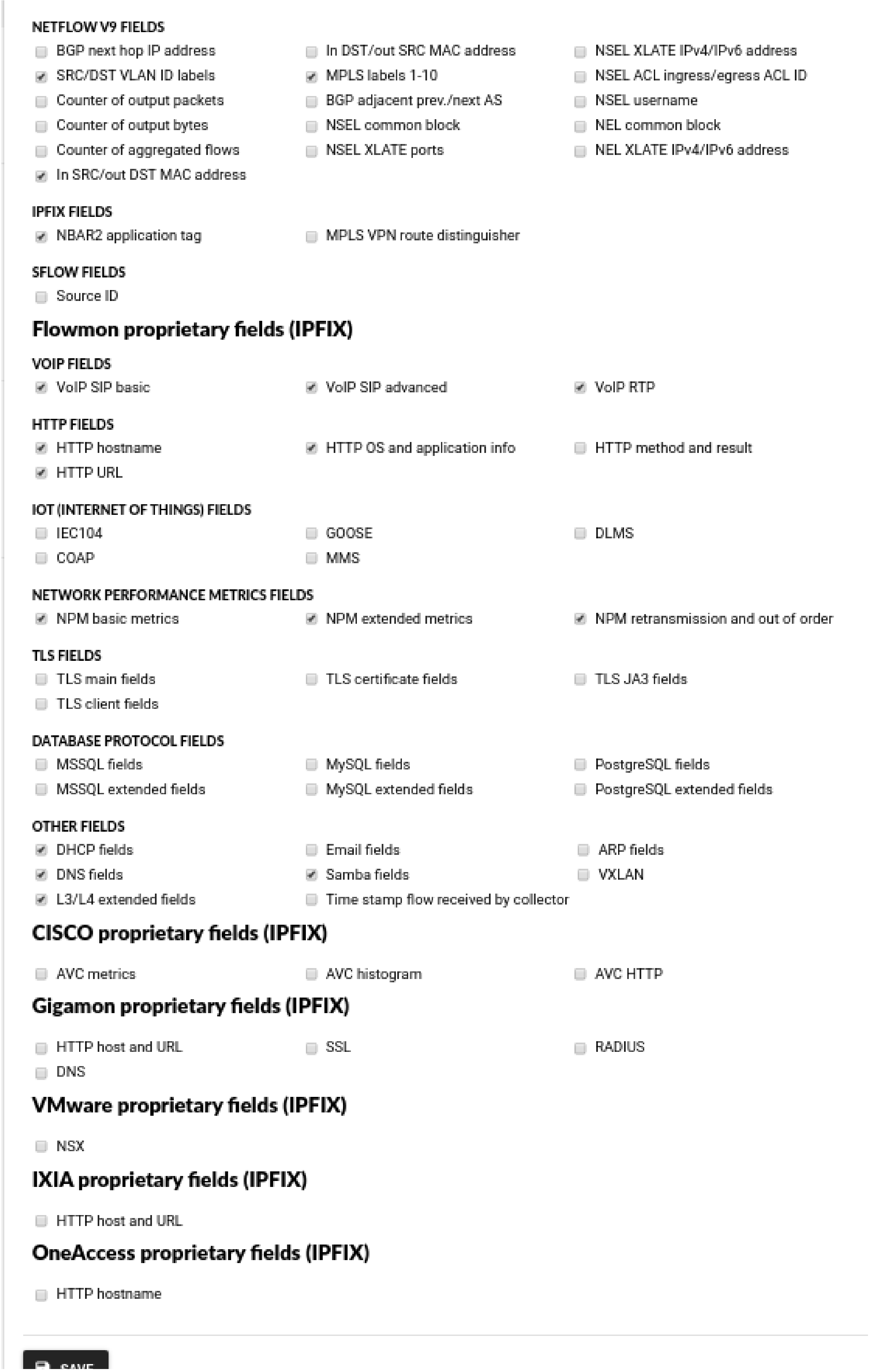
If there are some queries running in Flowmon Monitoring Center, button showing their count will appear. In some cases, very complicated queries over a large amount of data may take a very long time and slow down the device. It may be useful to kill these queries by pressing the **Kill running X FMC queries** button.

The **Clear data storage** button is used to clear the built-in collector database. This operation will irreversibly remove all stored NetFlow data. Depending on the size of stored NetFlow data this operation can take several minutes. During this time Monitoring center will not be accessible.

Built-in Collector - Flow database fields

On the Flow database fields page you can select which values are to be stored to flow database and process them in Flowmon Monitoring Center. Selected values must be present in the exported flows from probe or router. If not, they are filled with zeroes. Please keep in mind, that enabling a new value will increase the disk space necessary for store new flows. Description of the fields can be found on page [Flow Database Fields](#).





NETFLOW V9 FIELDS

- ☐ BGP next hop IP address
- ☑ SRC/DST VLAN ID labels
- ☐ Counter of output packets
- ☐ Counter of output bytes
- ☐ Counter of aggregated flows
- ☑ In SRC/out DST MAC address
- ☐ In DST/out SRC MAC address
- ☑ MPLS labels 1-10
- ☐ BGP adjacent prev./next AS
- ☐ NSEL common block
- ☐ NSEL XLATE ports
- ☐ NSEL XLATE IPv4/IPv6 address
- ☐ NSEL ACL ingress/egress ACL ID
- ☐ NSEL username
- ☐ NEL common block
- ☐ NEL XLATE IPv4/IPv6 address

IPFIX FIELDS

- ☑ NBAR2 application tag
- ☐ MPLS VPN route distinguisher

SFLOW FIELDS

- ☐ Source ID

Flowmon proprietary fields (IPFIX)

VOIP FIELDS

- ☑ VoIP SIP basic
- ☑ VoIP SIP advanced
- ☑ VoIP RTP

HTTP FIELDS

- ☑ HTTP hostname
- ☑ HTTP URL
- ☑ HTTP OS and application info
- ☐ HTTP method and result

IOT (INTERNET OF THINGS) FIELDS

- ☐ IEC104
- ☐ COAP
- ☐ GOOSE
- ☐ MMS
- ☐ DLMS

NETWORK PERFORMANCE METRICS FIELDS

- ☑ NPM basic metrics
- ☑ NPM extended metrics
- ☑ NPM retransmission and out of order

TLS FIELDS

- ☐ TLS main fields
- ☐ TLS client fields
- ☐ TLS certificate fields
- ☐ TLS JA3 fields

DATABASE PROTOCOL FIELDS

- ☐ MSSQL fields
- ☐ MSSQL extended fields
- ☐ MySQL fields
- ☐ MySQL extended fields
- ☐ PostgreSQL fields
- ☐ PostgreSQL extended fields

OTHER FIELDS

- ☑ DHCP fields
- ☑ DNS fields
- ☑ L3/L4 extended fields
- ☐ Email fields
- ☑ Samba fields
- ☐ Time stamp flow received by collector
- ☐ ARP fields
- ☐ VXLAN

CISCO proprietary fields (IPFIX)

- ☐ AVC metrics
- ☐ AVC histogram
- ☐ AVC HTTP

Gigamon proprietary fields (IPFIX)

- ☐ HTTP host and URL
- ☐ DNS
- ☐ SSL
- ☐ RADIUS

VMware proprietary fields (IPFIX)

- ☐ NSX

IXIA proprietary fields (IPFIX)

- ☐ HTTP host and URL

OneAccess proprietary fields (IPFIX)

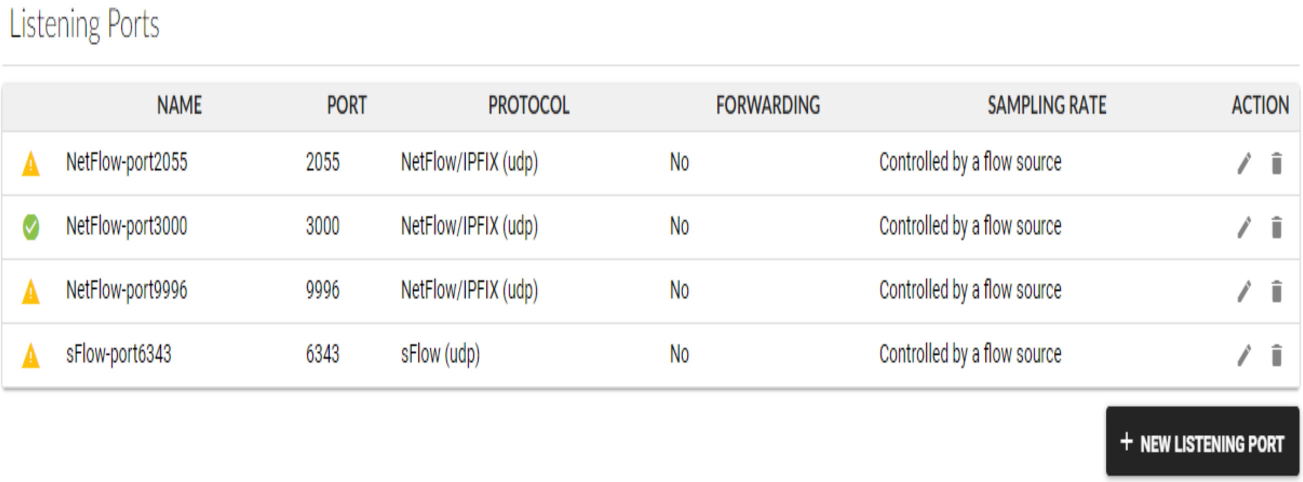
- ☐ HTTP hostname

Built-in Collector - Sources settings

On the Sources settings page, the limit for number of profiled sources and their interfaces can be configured. Please see the Sources chapter for more information.

Built-in Collector - Listening ports (Collector only)

In this page you can configure the listening ports for NetFlow, IPFIX, sFlow and other supported flow protocols and their forwarding. The listening port is defined by its name, port, network protocol and flow protocol. Please select the flow protocol used by your flow exporting device (router, probe). There are two options: NetFlow/IPFIX or sFlow. Option NetFlow/IPFIX applies also for all NetFlow clones like jFlow, NetStream etc. Please contact support@flowmon.com for more information about supported protocols.



Listening Ports

	NAME	PORT	PROTOCOL	FORWARDING	SAMPLING RATE	ACTION
⚠	NetFlow-port2055	2055	NetFlow/IPFIX (udp)	No	Controlled by a flow source	✎ 🗑
✓	NetFlow-port3000	3000	NetFlow/IPFIX (udp)	No	Controlled by a flow source	✎ 🗑
⚠	NetFlow-port9996	9996	NetFlow/IPFIX (udp)	No	Controlled by a flow source	✎ 🗑
⚠	sFlow-port6343	6343	sFlow (udp)	No	Controlled by a flow source	✎ 🗑

There is no need to define different listening ports for individual flow sources (Probes, routers, etc.) as Flowmon will automatically recognize and configure individual flow sources. It is recommend to keep default settings of listening ports unless there is a specific reason for defining additional listening port.

New listening port can be added by pressing button **New listening port**. A new form will appear.

Enter the name of listening port, port number, network protocol and flow protocol. If NetFlow/IPFIX is selected as flow protocol, TCP or UDP can be selected as network protocol. If TCP is selected, only IPFIX protocol is supported. For sFlow, only UDP is supported.

If TCP is selected as network protocol, the encryption TCP/TLS can be enabled. For TCP/TLS, the set of keys and certificates have to be generated for flow exporting device (monitoring port) and for collector. All certificates must be signed by the same certification authority (CA). Its certificate (CA certificate) must be provided together with collector key and certificate to each listening port using TCP/TLS protocol.

Sampling rate of received flow data is determined from flow protocol. It can be also defined statically (available for NetFlow only). For this purpose, check the **Define source sampling rate** and enter the number. If the entered value is positive, it is used only if the flow monitoring port does not provide the sampling rate information. If it provides the sampling rate, then this value is used. If you want to enforce your sampling rate, enter it as negative value.

Normally start time and end time of each flow is generated by flow source and included in flow data. However, some flow sources are not able to generate flow times and the flows are exported with no information about start time and end time. In this case, Flowmon Collector can generate the times itself based on the time of flow reception and active timeout defined on the flow source. The times will be generated as follows:

$t_{start} = reception\_time - active\_timeout$

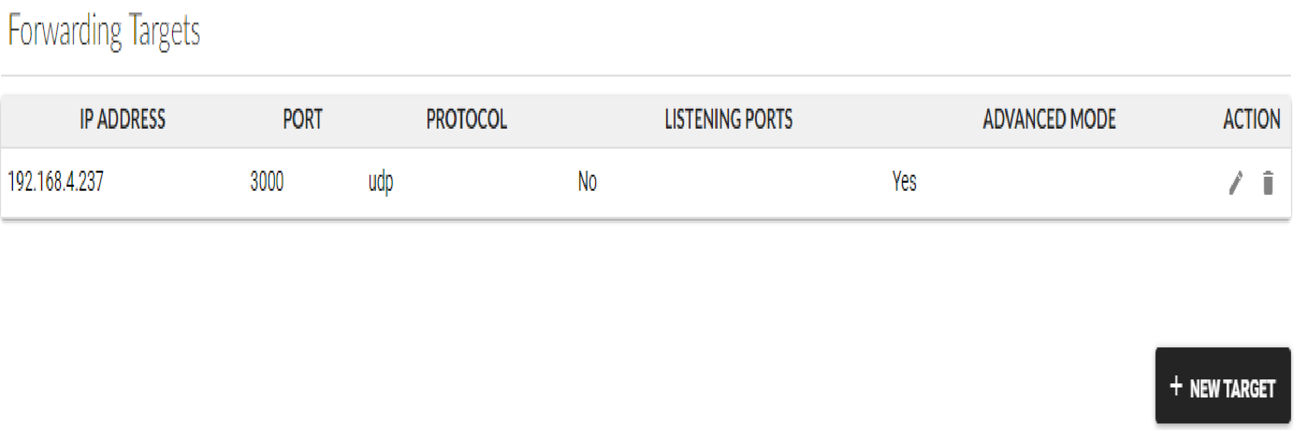
$t_{end} = reception\_time$

The generated times are only indicative. For long term flows, where active timeout applies, the flow duration is correct. The start time and end times are delayed a bit due to a time between ending the flow on flow source and its reception on Flowmon collector. For short flows where active timeout does not apply, the flow duration will be wrong. For enabling this feature, enable **Generate missing timestamps** switch and provide **Active timeout** of flow source sending data to this listening port.

Received flow data can be forwarded to multiple different targets. For this purpose, use **Forwarding targets** selector to choose forwarding targets for this Listening ports. The Forwarding targets must be configured in **Forwarding targets** page.

Built-in Collector - Forwarding targets (Collector only)

This section enables configuration of targets of forwarding of the listening ports. The configured forwarding targets are shown in the table below. Click the **New target** button or the **Edit** icon in the Action column to create a new forwarding target or to edit an existing one. This forwarding target will be applied to all listening ports selected in the **Listening ports** selector at the bottom of the page. Forwarding can be performed in two modes: **Compatible mode** and **Advanced mode**. These are available in separate tabs.



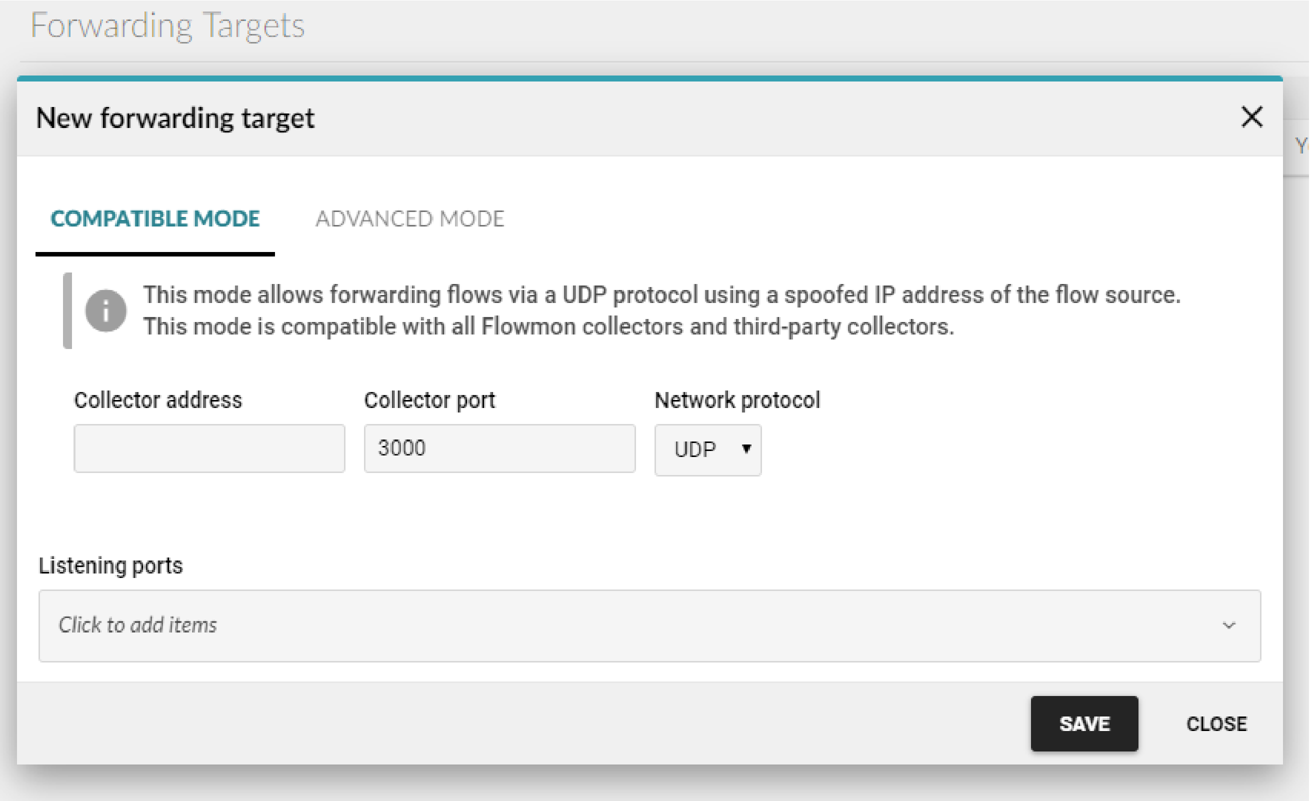
Forwarding Targets

IP ADDRESS	PORT	PROTOCOL	LISTENING PORTS	ADVANCED MODE	ACTION
192.168.4.237	3000	udp	No	Yes	✎ 🗑

Forwarding mode - compatible

This mode allows flow forwarding via UDP protocol with spoofed IP address of flow source. This mode is compatible with all Flowmon collectors and third party collectors. In compatible mode, the original IP address of flow source is preserved (i.e. IP spoof mode), so the target collector assigns the flows to the IP address of the original flow source. Please keep this in mind when configuring firewall rules etc.

In compatible mode, please enter IP address of collector and UDP port.


Forwarding Targets

New forwarding target

This mode allows forwarding flows via a UDP protocol using a spoofed IP address of the flow source. This mode is compatible with all Flowmon collectors and third-party collectors.

Collector address:

Collector port: 3000

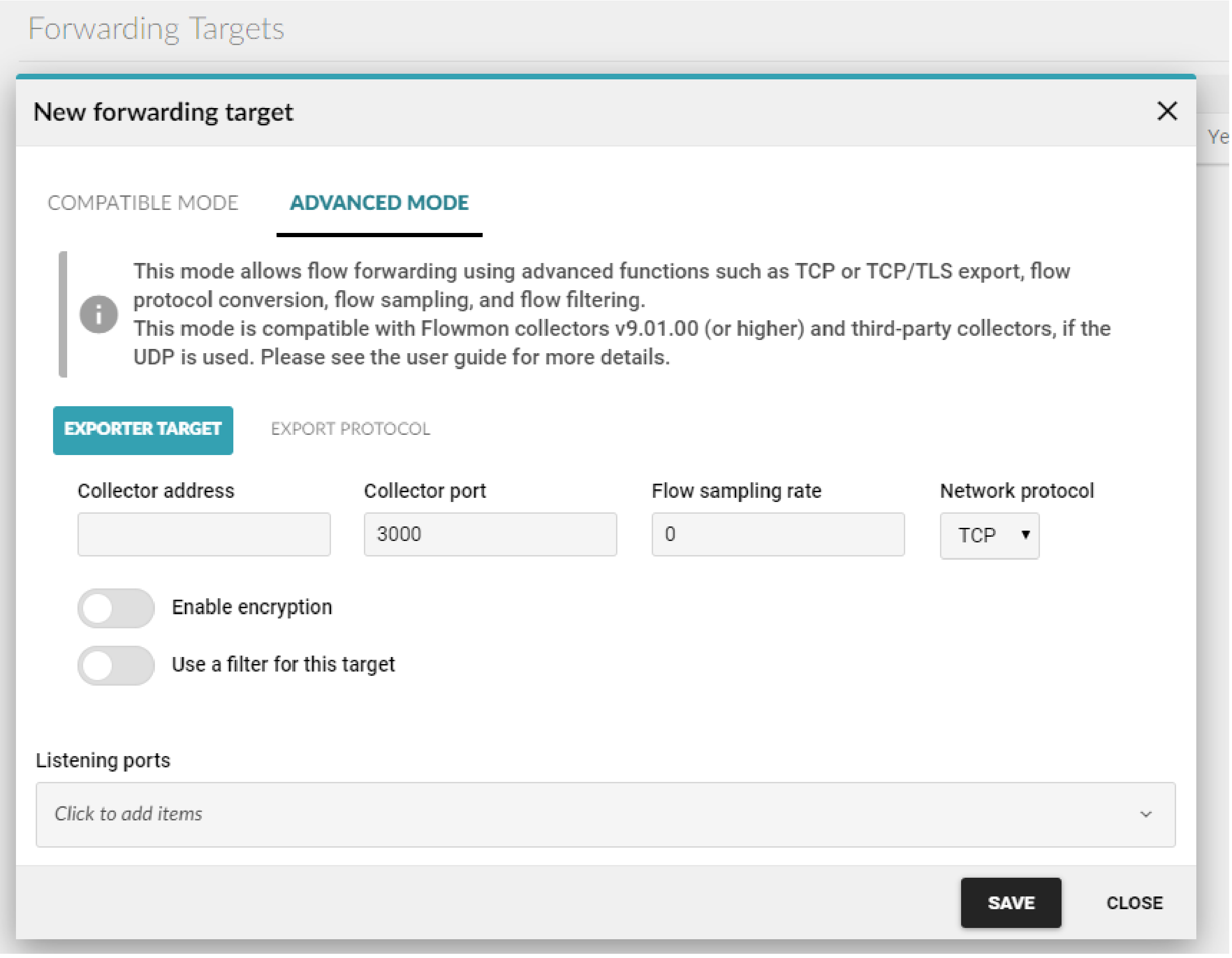
Network protocol: UDP

Listening ports: *Click to add items*

Forwarding mode - advanced

This mode allows flow forwarding using advanced capabilites such as TCP or TCP/TLS export, flow protocol conversion, flow sampling and flow filtering. This mode is compatible with Flowmon collectors v9.01.00 and higher.

In advanced mode there are two tabs - Export target and Export protocol.



This mode allows flow forwarding using advanced functions such as TCP or TCP/TLS export, flow protocol conversion, flow sampling, and flow filtering.
This mode is compatible with Flowmon collectors v9.01.00 (or higher) and third-party collectors, if the UDP is used. Please see the user guide for more details.

Collector address:
Collector port: 3000
Flow sampling rate: 0
Network protocol: TCP

○ Enable encryption
○ Use a filter for this target

Listening ports: *Click to add items*

In **Export target** tab, please enter IP address of target collector, port, flow sampling rate and choose transport protocol. TCP protocol is allowed only when IPFIX is used as an export protocol (see Export protocol tab). Moreover, the export filter can be added to define what flows will be forwarded to this target. For the filter syntax, please see section Syntax of Filter of Monitoring port. If TCP protocol is selected, the flow data can be forwarded encrypted using TCP/TLS protocol if the option **Enable encryption** is enabled. Then the collector private key, collector certificate and CA certificate must be provided.

In **Export protocol** tab, the flow export protocol can be selected out of options NetFlow v5, NetFlow v9 and IPFIX. For NetFlow v9 and IPFIX there is an option to change default template resending intervals.

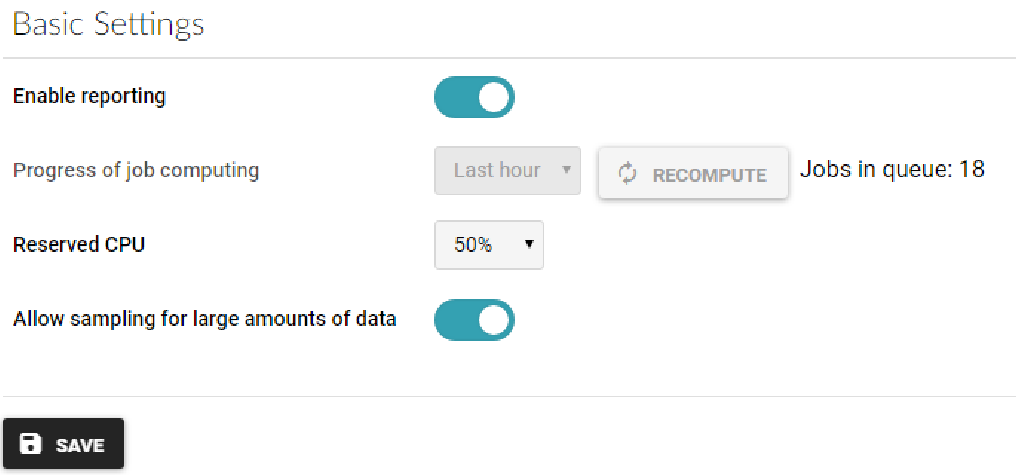
Press the **Save** button to apply changes. The entered values will be checked for loop presence which can be fatal for the collector. This operation can be more time consuming.

Reports' settings

Reports settings consists of **Basic settings**, **Remote storage**, **Working hours** and **Branding**.

Basic Settings

In basic settings, you can disable or enable reporting functionality. You are also allowed to recompute all chapters at once. Pick desired time interval and then click **Recompute** button. Progress of jobs computing shows, how many tasks are computed and how many task are waiting. **Reserved CPU** value says, how much CPU performance can be used to compute chapters statistics (done every hour). Option **Allow sampling for large amounts of data** is enabled in default configuration and allows the system to sample flow data during computation of reports if the amount of data is very big. So it speeds up the computation significantly and saves a lot of resources on heavily loaded collectors. The precisions of computed statistics is decreased only a little as for large amounts of data the sampled data are statistically unimportant. To save new value, press **Save** button.



Basic Settings

Enable reporting: on

Progress of job computing: Last hour — Jobs in queue: 18

Reserved CPU: 50%

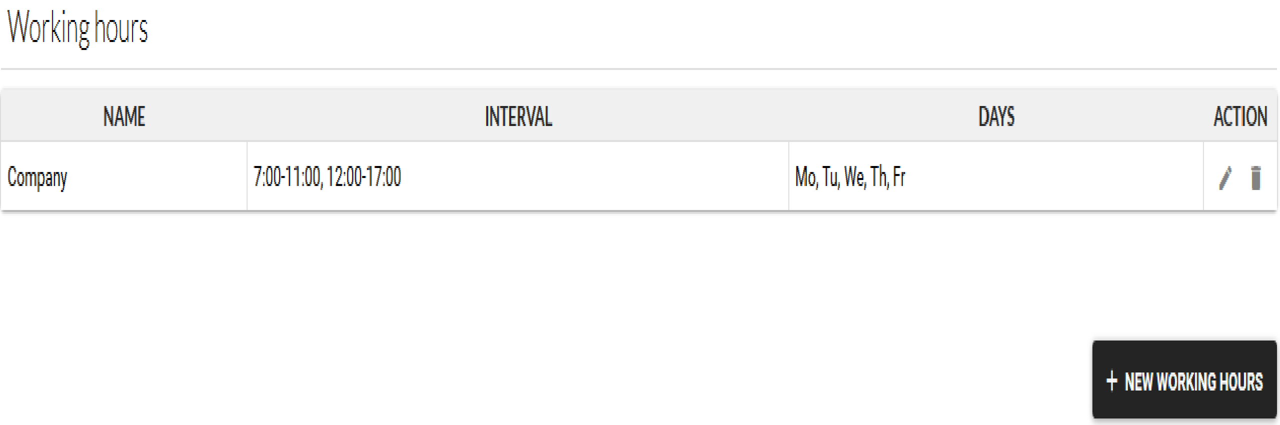
Allow sampling for large amounts of data: on

Reports settings - Basic settings

Working Hours

Here, you can set your company working hours. Then you will be able to reflect these settings in reports where statistics will be computed over these values.

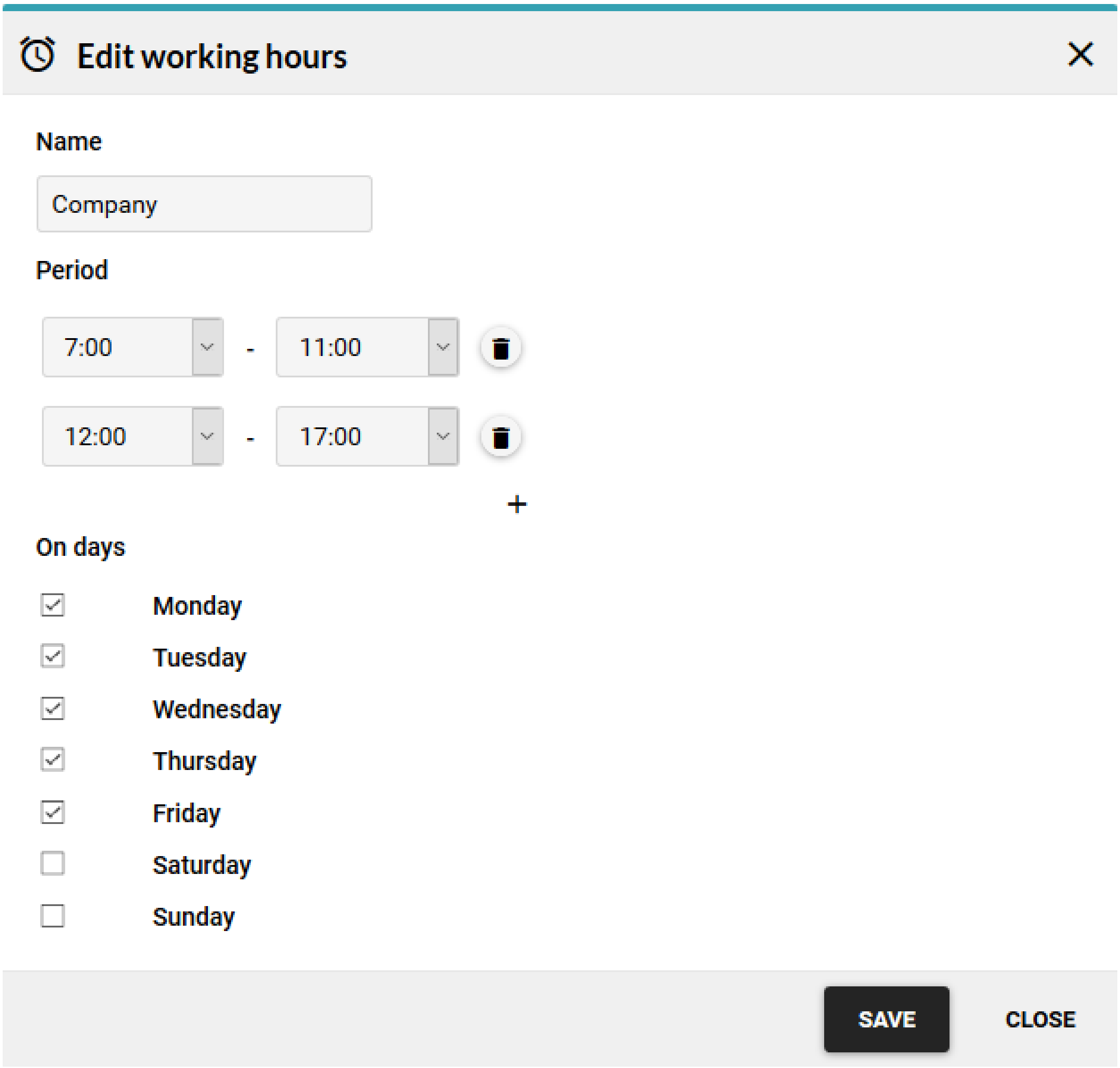
- **Name** - enter name for this entry
- **For interval** - pick times from and to up to four times. Mostly used only two intervals, gap for lunch time
- **On days** - select on which days are these time slots active



Working hours

NAME	INTERVAL	DAYS	ACTION
Company	7:00-11:00, 12:00-17:00	Mo, Tu, We, Th, Fr	

Working hours settings



Edit working hours

Name

Company

Period

7:00 - 11:00

12:00 - 17:00

On days

☑ Monday

☑ Tuesday

☑ Wednesday

☑ Thursday

☑ Friday

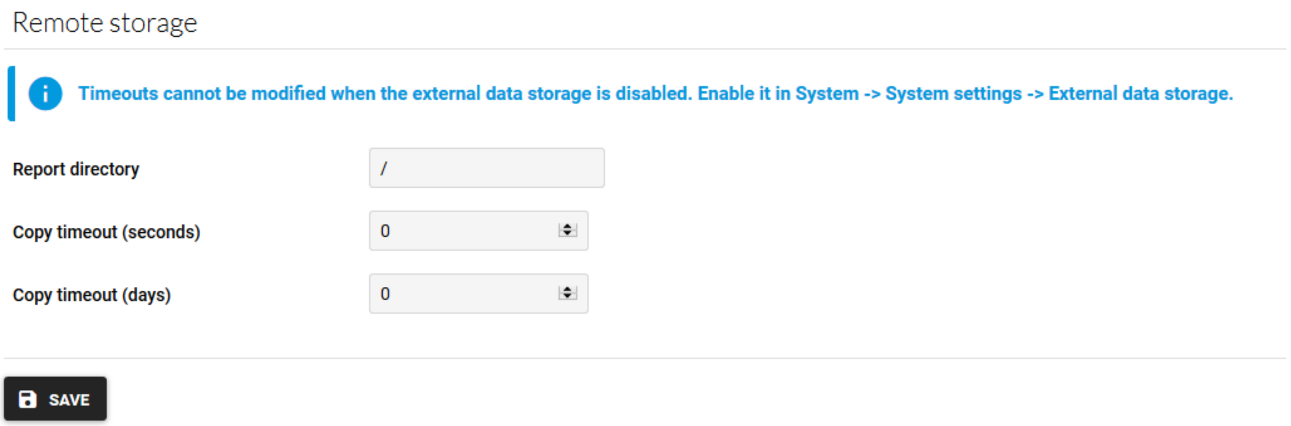
□ Saturday

□ Sunday

The Edit working hours dialogue

Remote Storage

In **Remote storage** parameters for storing reports to remote storage can be configured. Enter **Report directory**, where the reports will be copied. Item **Copy timeout** is used for specifying maximum time for copying of a single report. If the copy transaction takes longer, it is interrupted as unsuccessful. Use value zero for setting unlimited time. Item **Delete not copied files after** is used for configuration of maximum interval in days, when the older reports are removed from queue and system will not attempt to try to copy them again. Use value zero for setting unlimited time.



Remote storage

Timeouts cannot be modified when the external data storage is disabled. Enable it in System -> System settings -> External data storage.

Report directory	/
Copy timeout (seconds)	0
Copy timeout (days)	0

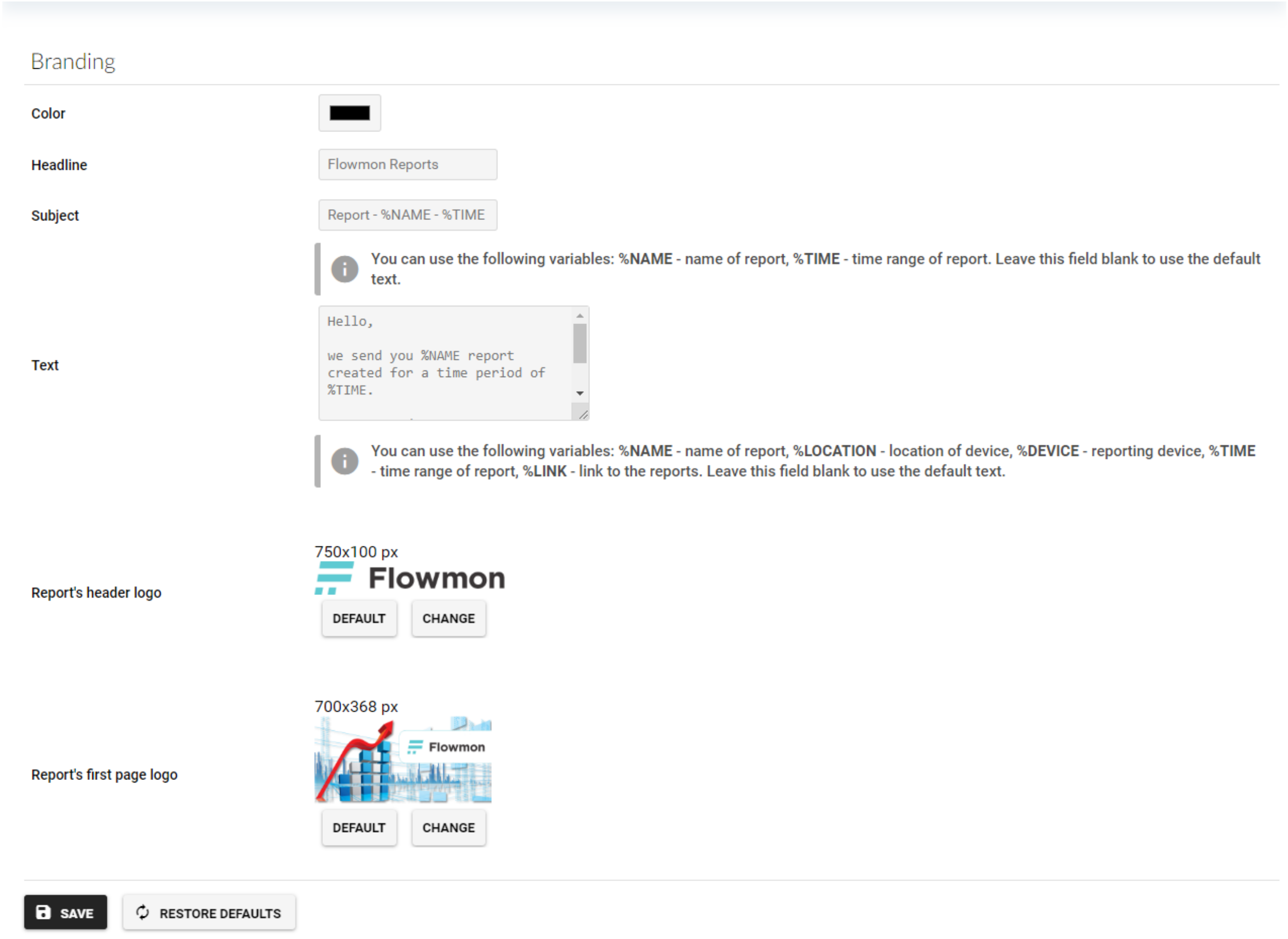
The Remote storage settings

Branding

In **Branding** you can specify the look of generated PDF reports. You can select main color, report name and email report subject and body. You can use macros here (described on the panel).

Note

You can delete data from reports in command line interface by command **/usr/bin/php /var/www/shtml/index.php Cli:ClearComputedReports**



Branding

Color	■
Headline	Flowmon Reports
Subject	Report - %NAME - %TIME

You can use the following variables: %NAME - name of report, %TIME - time range of report. Leave this field blank to use the default text.

Text:

```
Hello,

we send you %NAME report
created for a time period of
%TIME.
```

You can use the following variables: %NAME - name of report, %LOCATION - location of device, %DEVICE - reporting device, %TIME - time range of report, %LINK - link to the reports. Leave this field blank to use the default text.

Report's header logo: 750x100 px

Report's first page logo: 700x368 px

Flowmon branding options

Active Devices

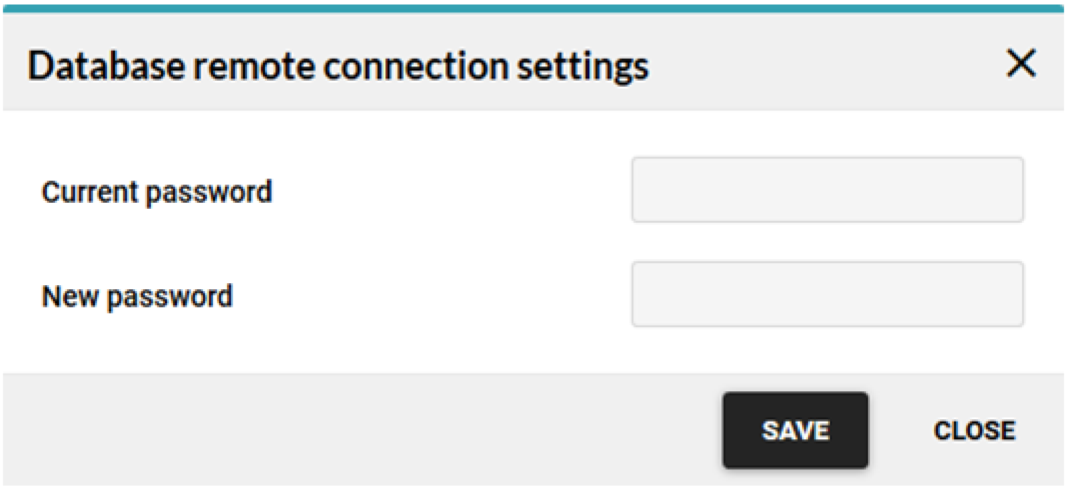
This page is used for configuration of Active Devices monitoring functionality. On some models, this function can be disabled by default. To enable it, it is necessary to enable the **Enable active devices logging** toggle switch and click the **Save** button to enable it.

Pick monitored flow sources from the selection menu. Only data from these sources will be collected. You can also specify a filter in case you want to monitor only specific traffic. Press **Save** button to save changes.

Database remote connection settings

Remote connection to PostgreSQL database can be configured by clicking the **Remote connection settings** button. Message in the frame shows firewall settings, whether PostgreSQL port 5432 can enabled or disabled. If you do not need to connect remotely to database, we recommend to disable this port. This can be done in **Remote access** page in Active firewall rules panel.

Below, there are two inputs that allow user to change password for the remote user of PostgreSQL database. Enter original password to Current password field and enter new password to New password field. Press **Save** button to perform change. You will be informed by message if the change was successful.

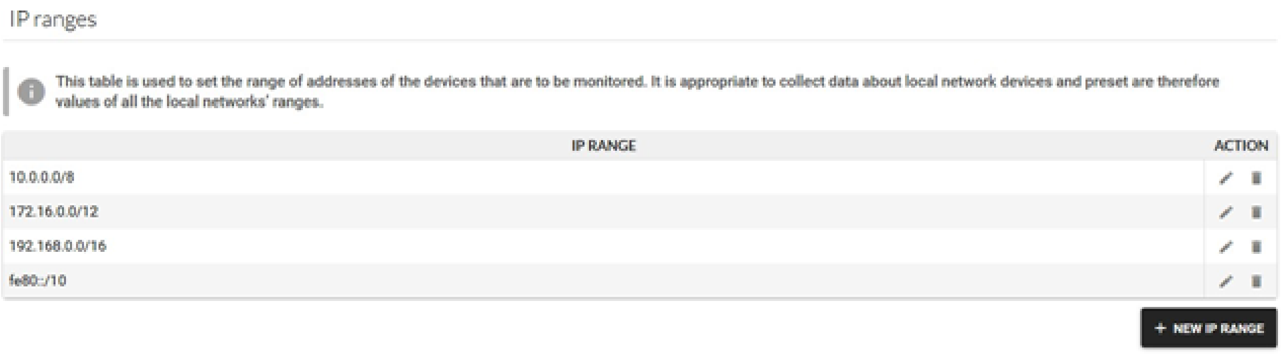


Remote access to database configuration

For remote access to database, use server address and port 5432. User login is **ipmac_cache_ro** and default password is **inv3a-t3ch**. Tables are stored in ipmac_cache schema. This user is allowed has only read-only permissions.

Active devices - IP ranges

The table **IP ranges** is used to configure all subnets in which the active devices are to be monitored. It makes sense to collect such in the local network and therefore there are preset values for all private and local networks: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, fe80::/10. To add new subnet, simply enter this value in the form **IP address/mask**.



IP ranges

This table is used to set the range of addresses of the devices that are to be monitored. It is appropriate to collect data about local network devices and preset are therefore values of all the local networks' ranges.

IP RANGE	ACTION
10.0.0.0/8	
172.16.0.0/12	
192.168.0.0/16	
fe80::/10	

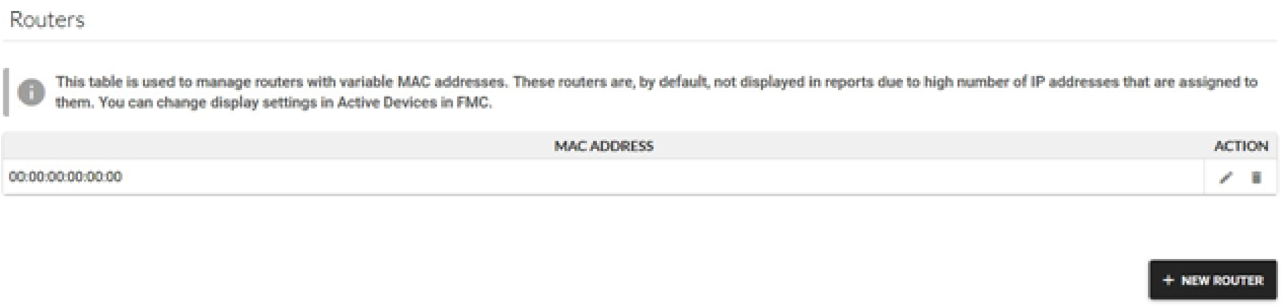
Active devices IP ranges configuration

Active devices - Routers

The **Routers** table is used to manage MAC addresses of routers which are hidden in reports by default, because they have normally assigned a large number of You can change your preference to show them in FMC in the search form.IP addresses.

Note

You can delete data from database of active devices in command line interface by command **/usr/bin/php /var/www/shtml/index.php Cli:ClearActiveDevices**



Routers

This table is used to manage routers with variable MAC addresses. These routers are, by default, not displayed in reports due to high number of IP addresses that are assigned to them. You can change display settings in Active Devices in FMC.

MAC ADDRESS	ACTION
00:00:00:00:00:00	

Routers configuration

AWS Flow Logs Converter

What is AWS Flow Logs Converter?

The AWS Flow Logs Converter is a configurable module of the Flowmon Monitoring Center (FMC).

It enables the user to collect, process and visualize AWS VPC Flow Logs (further referred to as flow logs) which contain information about the traffic captured in Amazon Virtual Private Cloud.

Brief Implementation Description

The flow logs are periodically acquired from Amazon CloudWatch, processed, converted to IPFIX format and subsequently sent to Flowmon Collector to a defined UDP port.

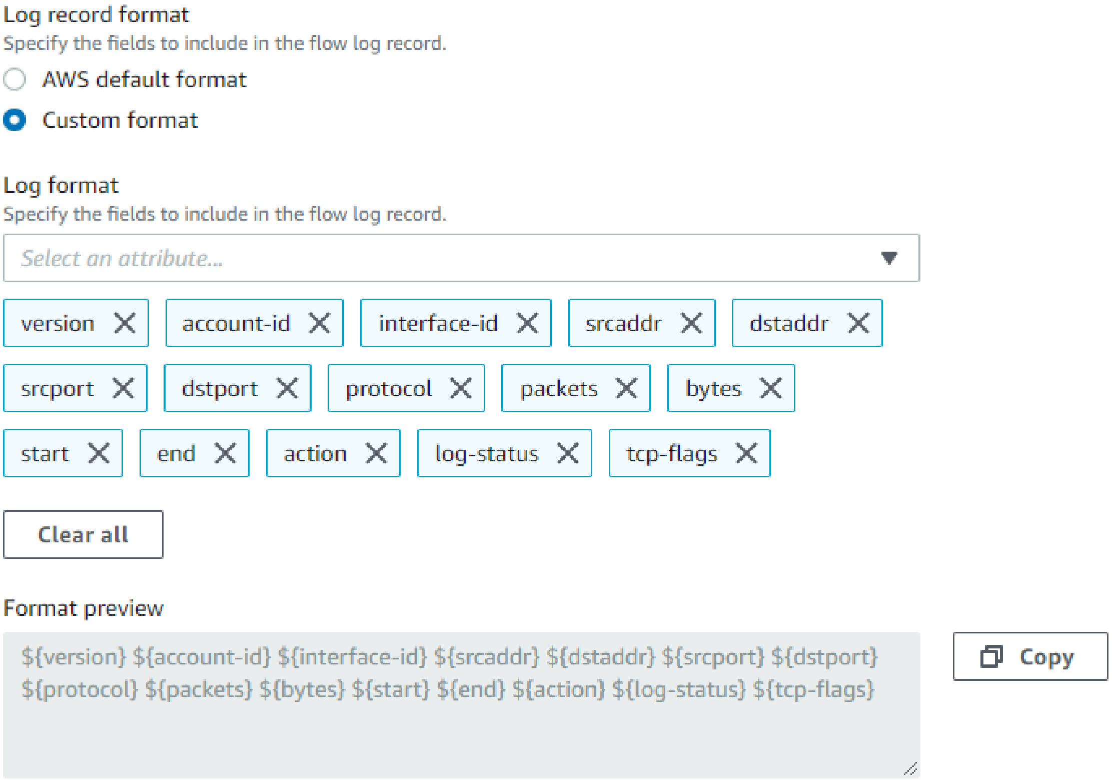
Flowmon Collector treats data from this port as regular flows recovered from any other port.

Setting Up Flow Logs for a VPC

To set up the flow logs in your cloud and forward them to AWS CloudWatch, please follow the instructions specified here. It is important that every flow log stream contains flow logs from one interface only.

The AWS Flow Logs Converter can process TCP flags which are not enabled in AWS VPC Flow Logs by default. To enable TCP flags processing, it is necessary to specify a c**ustom format** of the **Log Record** when creating a new Flow Log.

The custom format must contain the following fields in the following order:



Log record format
Specify the fields to include in the flow log record.

○ AWS default format
● Custom format

Log format
Specify the fields to include in the flow log record.

Select an attribute...

version ✕ account-id ✕ interface-id ✕ srcaddr ✕ dstaddr ✕
srcport ✕ dstport ✕ protocol ✕ packets ✕ bytes ✕
start ✕ end ✕ action ✕ log-status ✕ tcp-flags ✕

Clear all

Format preview

```
${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr} ${srcport} ${dstport}
${protocol} ${packets} ${bytes} ${start} ${end} ${action} ${log-status} ${tcp-flags}
```

Copy

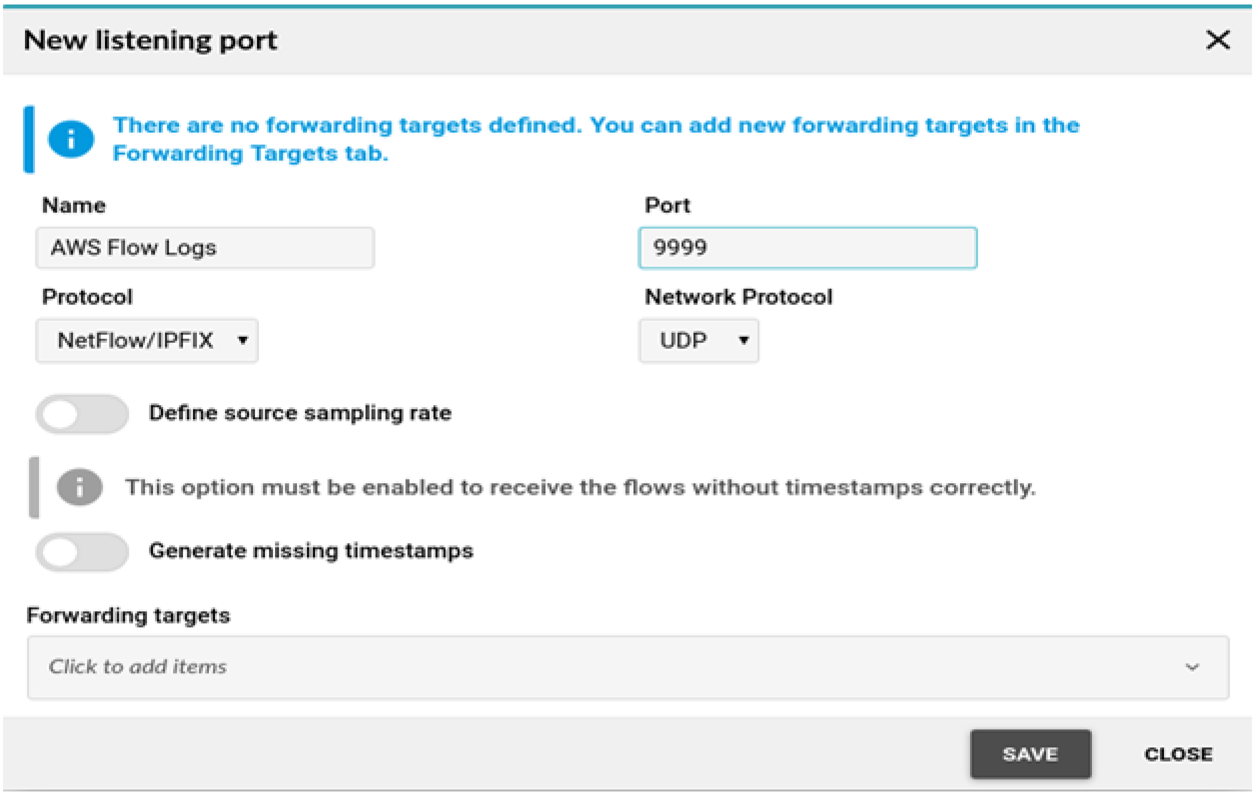
The AWS Flow Logs Converter can process only the default Flow Record format and the custom format specified above.

Setting Up Flow Logs in Flowmon Configuration Center

To start receiving flow logs in Flowmon Monitoring Center, follow the following instructions:

Step 1: Create a new listening port in **Configuration Center -> FMC Configuration -> Listening Ports**

The name and port number of the new listening port can be chosen as needed. However, the network protocol must be **UDP** and the format of the transferred data must be **NetFlow/IPFIX**.



New listening port

There are no forwarding targets defined. You can add new forwarding targets in the Forwarding Targets tab.

Name: AWS Flow Logs

Port: 9999

Protocol: NetFlow/IPFIX

Network Protocol: UDP

Define source sampling rate

This option must be enabled to receive the flows without timestamps correctly.

Generate missing timestamps

Forwarding targets: Click to add items

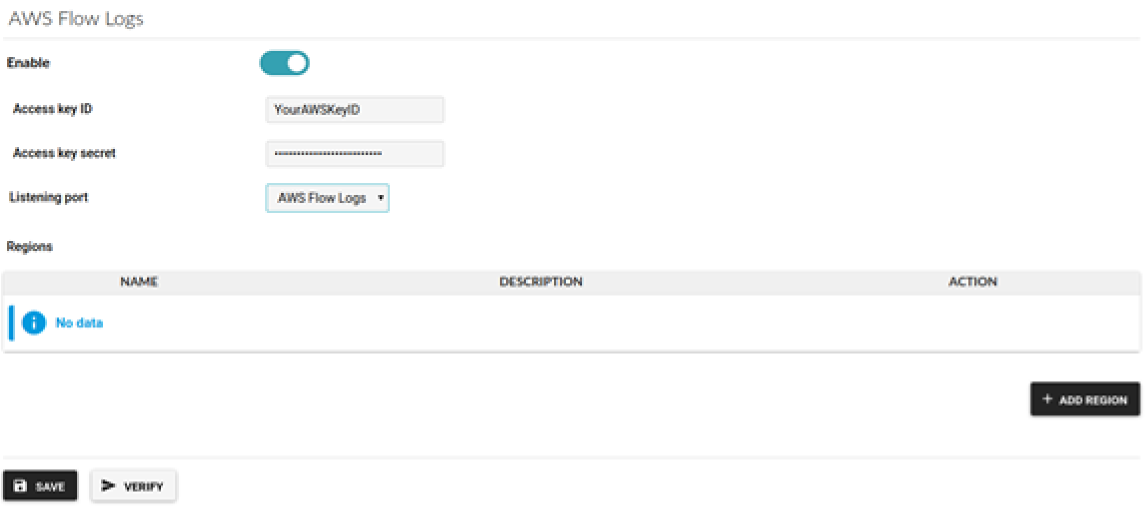
Addition of a listening port

Step 2: Configure the access information, regions and log groups from which the flow logs will be retrieved.

Configuration Center -> FMC Configuration -> AWS Flow Logs

The *access key ID* and the *secret access key* are mandatory credentials provided by Amazon.

Select the previously configured listening port.



AWS Flow Logs

Enable

Access key ID: YourAWSKeyID

Access key secret: ••••••••••••••••••••••

Listening port: AWS Flow Logs

Regions

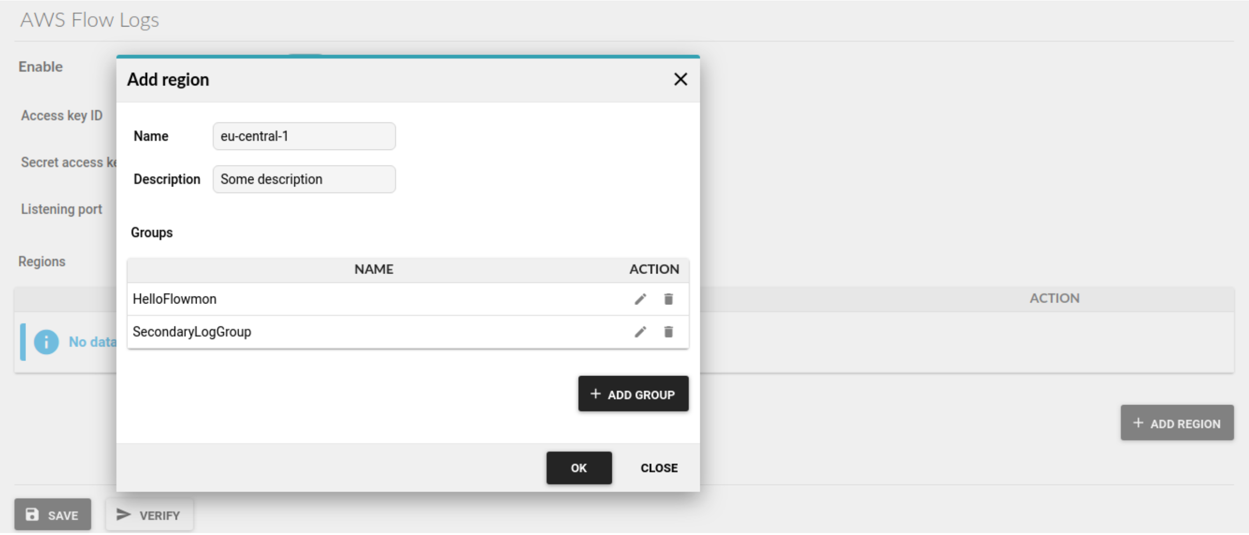
NAME	DESCRIPTION	ACTION
No data		

Acquiring log information

Click the **Add Region** button to configure the endpoints where the flow logs should be retrieved.

Insert the name of the region (without availability zone) in which your flow logs are physically stored. List of all possible regions can be found here. Note that the region **Name** field is expected to contain values like *eu-central-1* rather than *EU (Frankfurt)*. It is also possible to define short description of the region.

Lastly, it is necessary to provide at least one log group (by clicking the **Add group** button and filling in the name). All flow log streams in the provided group will be processed and every stream will be shown as a unique interface of the log group in the **Monitoring Center**.



Name: eu-central-1

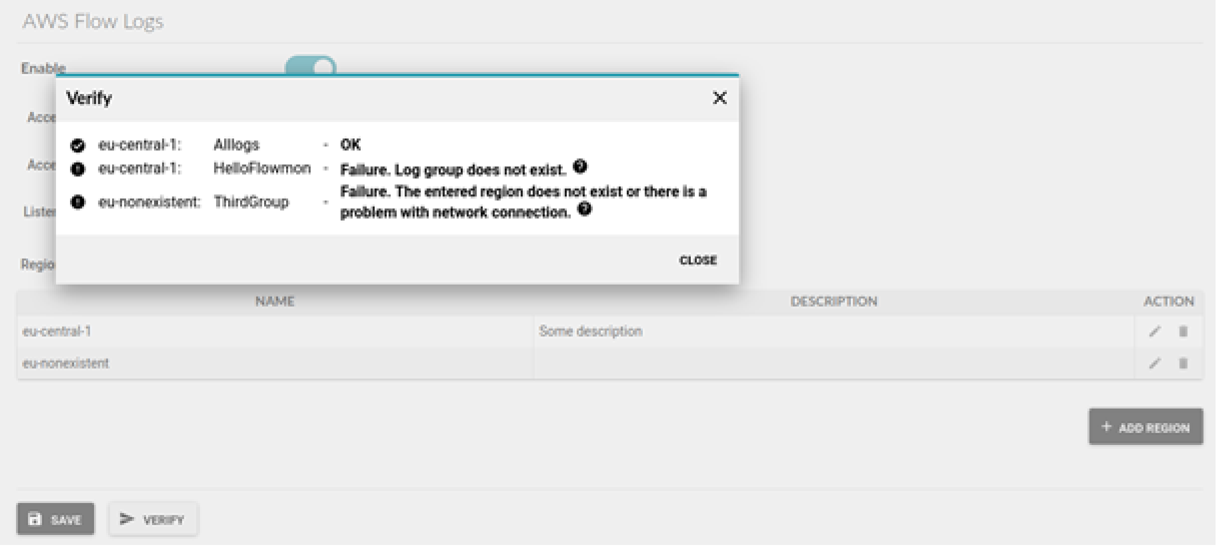
Description: Some description

Groups

NAME	ACTION
HelloFlowmon	
SecondaryLogGroup	

The provided configuration can be optionally verified by clicking the **Verify** button. This will check whether the FMC is able to connect to the specified log groups using the provided AWS credentials.

Note that the provided configuration undergoes the verification process every time the **Save** button is clicked.



```
eu-central-1:     Alllogs       - OK
eu-central-1:     HelloFlowmon  - Failure. Log group does not exist.
eu-nonexistent:   ThirdGroup    - Failure. The entered region does not exist or there is a
                                  problem with network connection.
```

NAME	DESCRIPTION	ACTION
eu-central-1	Some description	
eu-nonexistent		

Verification

Newly created configuration must be saved (by clicking the **Save** button). This will start the process of retrieving the Flow logs. To stop the process of retrieving, disable it and click the **Save** button.

Viewing VPC Flow Logs in Monitoring Center

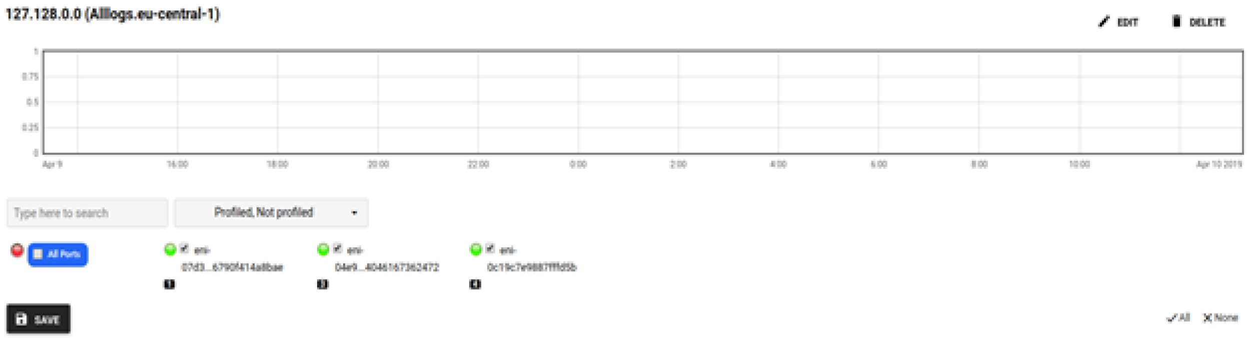
It can take up to 20 minutes (see the limitations) before first flow logs can be visualized.

Every log group has internally assigned a unique IP address (from subnet 127.128.0.0/16) and is treated as a unique flow source.

All sources can be found in **Flowmon Monitoring Center -> Sources.**

Click the **Profile** button to see traffic of the individual streams.

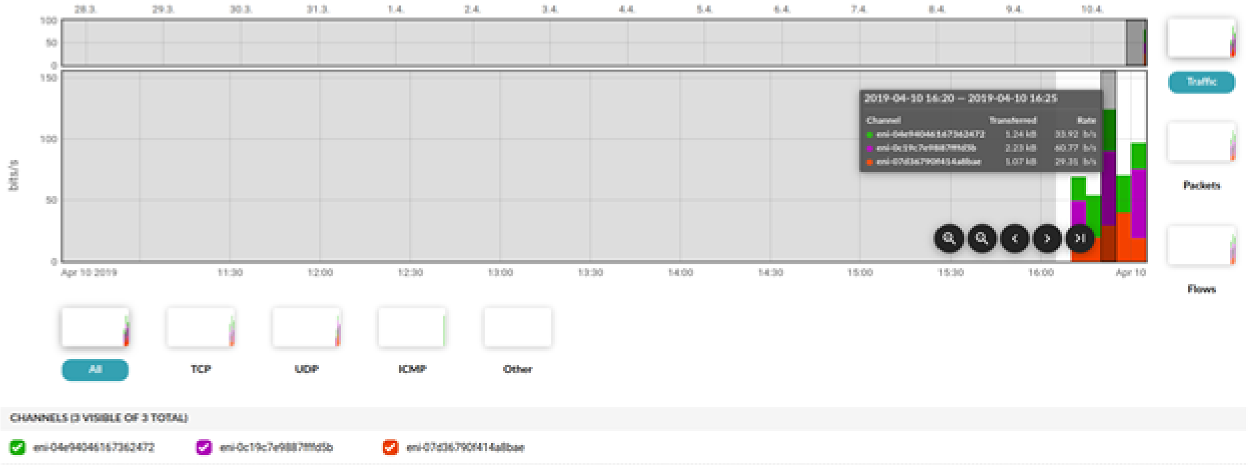
Select all available streams and click the **Save** button.



Sources

Switch to: **Flowmon Monitoring Center -> Profiles -> Sources ->** ***Your Log Group***

It is possible to view and analyze flows from flow logs as if they were flows from regular data sources.



2019-04-10 16:20 – 2019-04-10 16:25

Channel	Transferred	Rate
🟩 eni-04e940461673624 72	1.24 kB	33.92 b/s
🟪 eni-0c19c7e9887fffd5b	2.23 kB	60.77 b/s
🟧 eni-07d36790f414a8bae	1.07 kB	29.31 b/s

CHANNELS (3 VISIBLE OF 3 TOTAL)

☑ eni-04e9404046167362472 ☑ eni-0c19c7e9887fffd5b ☑ eni-07d36790f414a8bae

Flow Log Vizualization

Limitations of Flow Logs

There are some limitations which stem from the flow logs themselves that need to be taken into account.

- If your network interface has multiple IPv4 addresses and traffic is sent to a secondary private IPv4 address, the flow log displays the primary private IPv4 address in the destination IP address field.
- If traffic is sent to an ENI and the destination is not any of the ENI IP addresses, the flow log displays the primary private IPv4 address in the destination IP address field.
- If traffic is sent from an ENI and the source is not any of the ENI IP addresses, the flow log displays the primary private IPv4 address in the source IP address field.
- If traffic is sent to or sent by a network interface, the flow log always displays the primary private IPv4 address, regardless of the packet source or destination, in the interface IP address field.

Flow logs do not capture all IP traffic. The following types of traffic are not logged:

- Traffic generated by instances when they contact the Amazon DNS server. If you use your own DNS server, then all traffic heading to that DNS server is logged.
- Traffic generated by a Windows instance for activation of the Amazon Windows license.
- Traffic to and from 169.254.169.254 for the instance metadata.
- Traffic to and from 169.254.169.123 for the Amazon Time Sync service.
- DHCP traffic.
- Traffic to the reserved IP address for the default VPC router. For more information, see VPC and Subnet Sizing.

- Traffic between an endpoint network interface and a Network Load Balancer network interface. For more information, see VPC Endpoint Services (AWS PrivateLink).
- Some flow log records might get skipped during the capture window. This may be because of an internal capacity constraint, or an internal error.

Furthermore, the delay between the time when the traffic actually occurred and the time it can be seen in Monitoring Center can reach up to 20 minutes in the worst case scenario, however; the delay will get smaller with a higher amount of traffic volume present in the monitored cloud.

This is caused by the 10-15 minutes capture window in which the packets are aggregated to the flow logs before being published, and by the subsequent 5 minutes delay before Flowmon Collector closes the current profile and shows the traffic in the GUI.

Flowmon Collector stores incoming flows to a currently opened profile, and therefore it is advised to select multiple adjacent profiles when searching for flows in a particular time.

Google Cloud Flow Logs

Flowmon Collector is capable of processing and visualizing Google Cloud VPC Flow Logs. Google Cloud VPC Flow Logs (further referred to as flow logs) are records of network connections between VM instances in VPC networks. Flowmon Collector acquires flow logs by polling on Google Cloud Pub/Sub subscription.

Setting Up Google Cloud VPC Flow Logs

Follow the official instructions to enable generating flow logs for certain subnets in your VPC.

It is important to mention several configurable options during the configuration of flow logs:

- Aggregation Interval: *5 minutes* - recommended (standard configuration of Flowmon probes also use the 5-minute aggregation interval)
- **Include metadata: *On* - mandatory** (necessary to display information about the VPC and subnets in FMC)
- Sample Rate: *100* - recommend in order to obtain all flow logs

Configuring Google Cloud Pub/Sub Subscription

Google Cloud Pub/Sub subscription must follow certain criteria so it can be utilized efficiently by Flowmon Collector.

The recommended configuration of a subscription to maximize the performance and minimize the cost:

- **Delivery type: *Pull* - mandatory**
- Message retention duration: *1 hour*
- Retain acknowledged messages: *No*
- Acknowledgement deadline: *10 seconds*
- Message ordering: *No*
- Dead lettering: *No*
- Retry policy: *Retry immediately*

Flowmon Collector uses Google Cloud Service Account Key (in JSON format) for authentication when acquiring flow logs from the Google Cloud Pub/Sub subscription. The service account used for acquiring flow logs must include the *Pub/Sub Subscriber* role in Google Cloud IAM. Note that such service account can access any Pub/Sub subscriptions with a Google Cloud project. For more information about setting up permissions, please refer to the official guide.

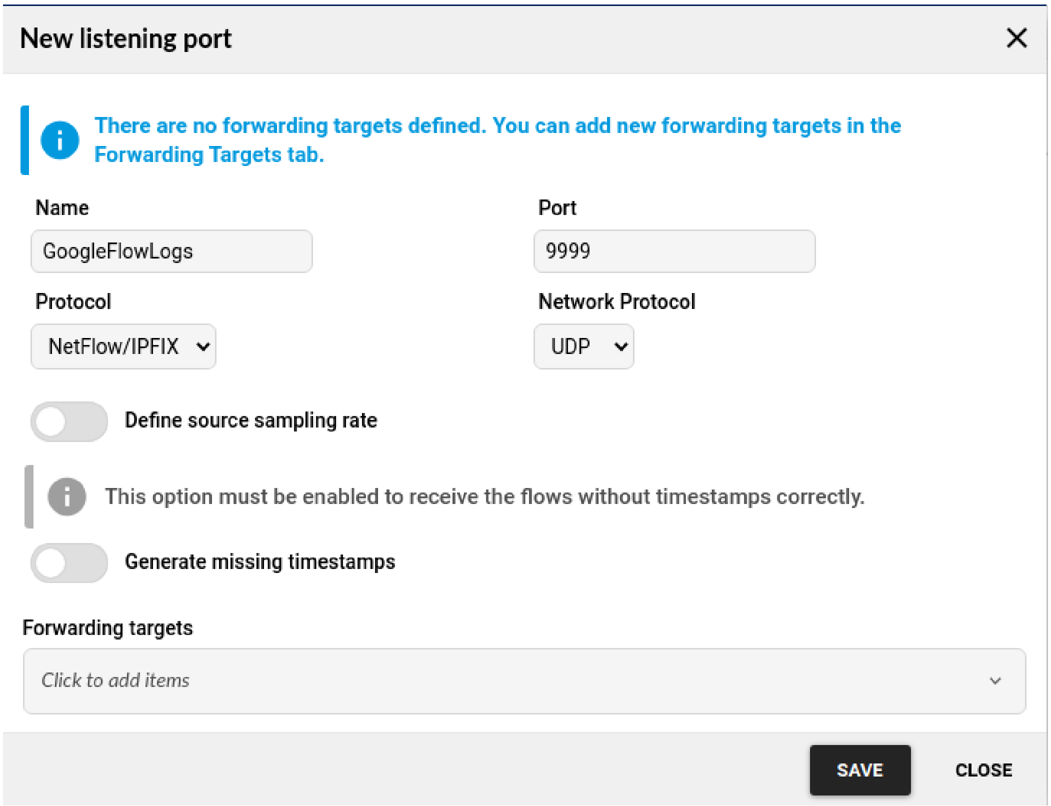
Setting Up Google Cloud VPC Flow Logs Processing

To start receiving flow logs in Flowmon Monitoring Center, follow the following instructions:

Step 1: Create a new listening port in **Configuration Center -> FMC Configuration -> Listening Ports**

The name and port number of the new listening port can be chosen as needed. However, the network protocol must be **UDP** and the format of the transferred data must be **NetFlow/IPFIX**.

Optionally, you can define source sampling rate of this listening port, because Google Cloud already samples packets that leave and enter a VM to generate flow logs. Not every packet is captured into its own log record. About **1 out of every 10** packets is captured, but this sampling rate might be lower depending on the VM's load. You cannot adjust this rate.



New listening port

There are no forwarding targets defined. You can add new forwarding targets in the Forwarding Targets tab.

Name: GoogleFlowLogs

Port: 9999

Protocol: NetFlow/IPFIX

Network Protocol: UDP

○ Define source sampling rate

This option must be enabled to receive the flows without timestamps correctly.

○ Generate missing timestamps

Forwarding targets: Click to add items

Step 2: Enable processing of the Google Cloud Flow Logs and configure individual subscriptions.

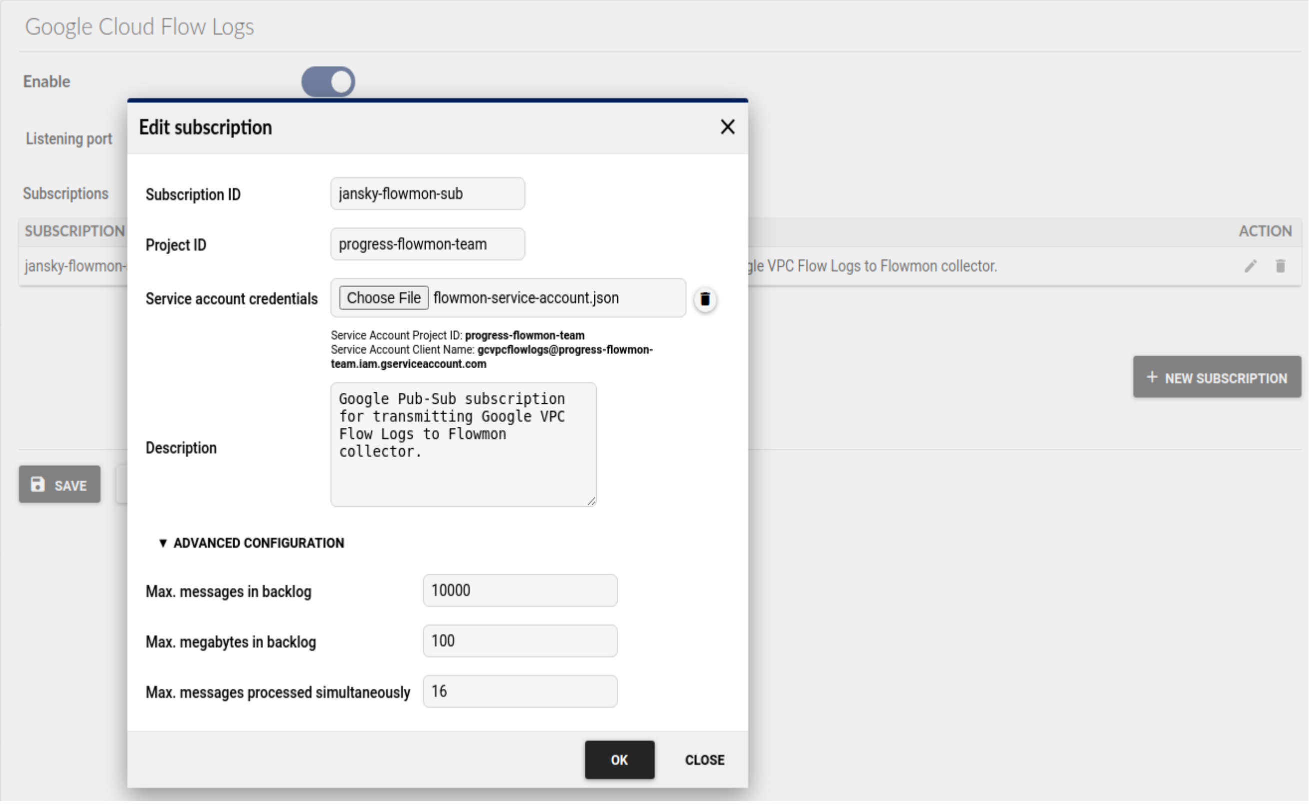
Navigate to: **Configuration Center -> FMC Configuration -> Google Cloud Flow Logs**

Toggle the **Enable** button and select the previously created **Listening port** from the drop-down menu.

Click the **New Subscription** button which allows you to configure a list of *Google Cloud Pub/Sub subscriptions* from which flow logs will be obtained and processed. The following parts of a subscription can be configured:

- *Subscription ID* - ID of the Google Cloud Pub/Sub subscription
- *Project ID* - ID of the Google Cloud project to which the subscription belongs
- *Service account credentials* - Google Cloud Service Account Key in JSON format, with permissions to subscribe to the Pub/Sub subscription. Follow the official instructions to create the key.

- *Description* - custom description of the subscription
- *Advanced Configuration* - several options which can affect performance of the subscription process at the cost of increased resources consumption
    - *Max. messages in backlog* - the maximal number of Pub/Sub messages which can be in queue for processing (not recommended to set below 1000 messages).
    - *Max. megabytes in backlog* - the maximal number of bytes which can be in queue for processing (it is recommended to respect the size of messages containing flow logs - not more than several KB per message)
    - *Max. messages processed simultaneously* - number of parallel background workers for polling flow logs from the Pub/Sub subscription. It is recommended to set this value as low as possible based on the expected number of the processed Pub/Sub messages per second. The range is limited to **2** - **16** possible workers (it is recommended to use a power of 2). Two workers can handle processing around **100,000 Pub/Sub messages per second** (tested on a **c2-standard-16** computing instance). Keep in mind that configuring several subscriptions on the same appliance lowers the performance in general. It is **not recommended** to use more than 32 background workers in total across all configured subscriptions.



Edit subscription ×

Subscription ID: jansky-flowmon-sub

Project ID: progress-flowmon-team

Service account credentials: Choose File flowmon-service-account.json

Service Account Project ID: **progress-flowmon-team**
Service Account Client Name: **gcvpcflowlogs@progress-flowmon-team.iam.gserviceaccount.com**

Description:

```
Google Pub-Sub subscription
for transmitting Google VPC
Flow Logs to Flowmon
collector.
```

▼ ADVANCED CONFIGURATION

Max. messages in backlog: 10000

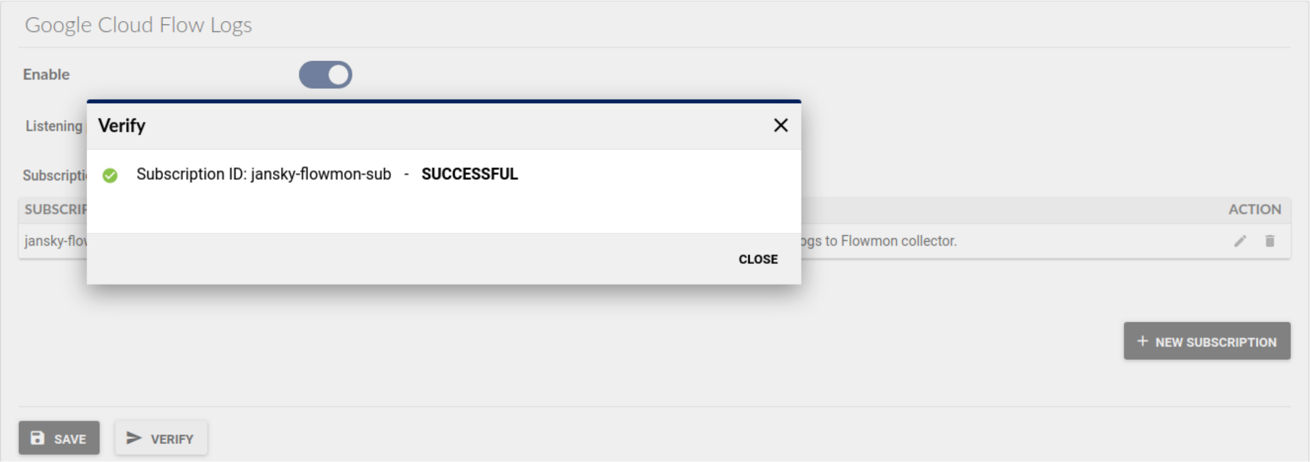
Max. megabytes in backlog: 100

Max. messages processed simultaneously: 16

OK CLOSE

The provided configuration can be optionally verified by clicking the **Verify** button. This will check whether the FMC is able to connect to the specified Pub/Sub subscriptions using the provided Service account credentials.

Note that the provided configuration undergoes the verification process every time the **Save** button is clicked.


Google Cloud Flow Logs

Enable

Listening

Subscripti

SUBSCRIP

jansky-flo

ogs to Flowmon collector.

ACTION

Verify

Subscription ID: jansky-flowmon-sub - **SUCCESSFUL**

Viewing VPC Flow Logs in Monitoring Center

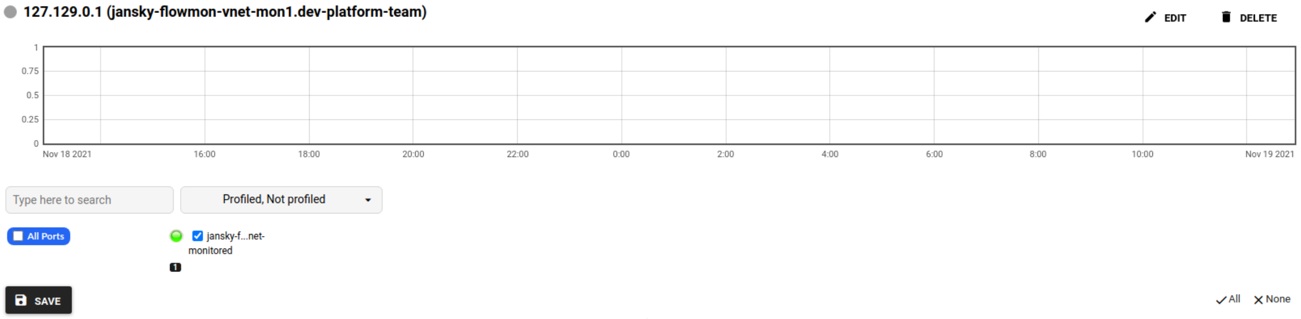
Multiple flow sources are created when using Google Cloud VPC Flow Logs. Each flow source is internally assigned a unique IP address (from subnet 127.129.0.0/16) and its name corresponds to a VPC inside a Google Cloud project in a format: **vpc-name.project-id**.

All sources can be found in **Flowmon Monitoring Center -> Sources.**

Click the **Profile** button if you want to divide the flow source into separate channel. Each channel corresponds to a subnet inside the VPC and is uniquely distinguishable by the subnet name.

Select all available subnets and click the **Save** button.

It is possible to view and analyze the flows from the flow logs as if they were flows from regular data sources.


127.129.0.1 (jansky-flowmon-vnet-mon1.dev-platform-team)

Profiled, Not profiled

☑ jansky-f...net-monitored

Azure Flow Logs

Flowmon Collector is capable of processing and visualizing Azure NSG Flow Logs. Azure NSG Flow Logs (further referred to as flow logs) are sampled records of the network flow sent from and received by VM instances. Flow logs is a feature provided by the *Network Watcher* service and dependent on the *Microsoft Insights* resource provider. Flowmon Collector periodically connects to the configured Azure Blob Storage containers and downloads newly added flow logs. The flow logs are subsequently converted to the IPFIX format and can be viewed in Flowmon Monitoring Center (FMC).

Setting Up Azure NSG Flow Logs

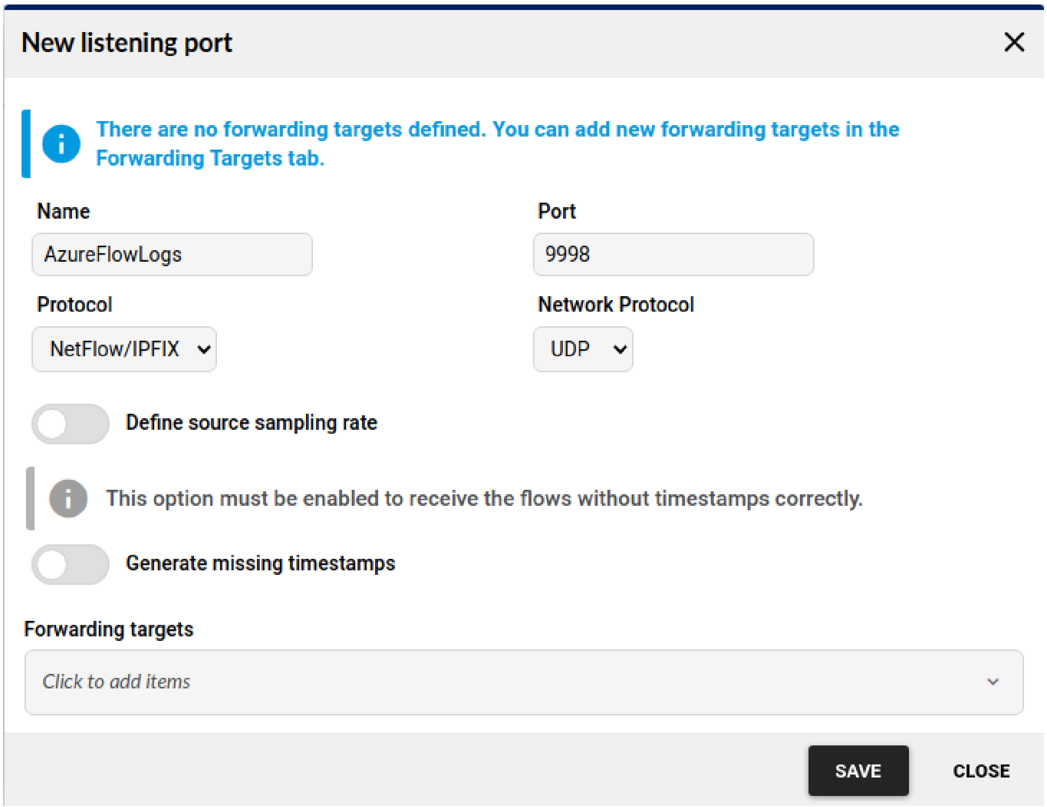
Follow the official instructions to enable collecting of flow logs in Azure Blob Storage for your virtual machines.

Setting Up Azure NSG Flow Logs Processing

To start receiving flow logs in FMC, follow the following instructions:

Step 1: Create a new listening port in **Configuration Center -> FMC Configuration -> Listening Ports**

The name and port number of the new listening port can be chosen as needed. However, the network protocol must be **UDP** and the format of the transferred data must be **NetFlow/IPFIX**.



New listening port

There are no forwarding targets defined. You can add new forwarding targets in the Forwarding Targets tab.

Name: AzureFlowLogs

Port: 9998

Protocol: NetFlow/IPFIX

Network Protocol: UDP

Define source sampling rate

This option must be enabled to receive the flows without timestamps correctly.

Generate missing timestamps

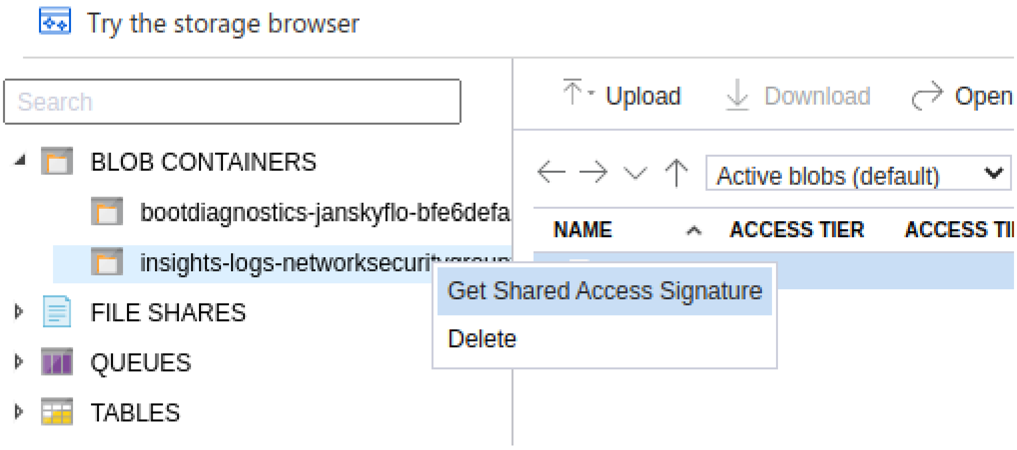
Forwarding targets: *Click to add items*

Step 2: Enable processing of the Azure NSG Flow Logs and configure individual subscriptions.

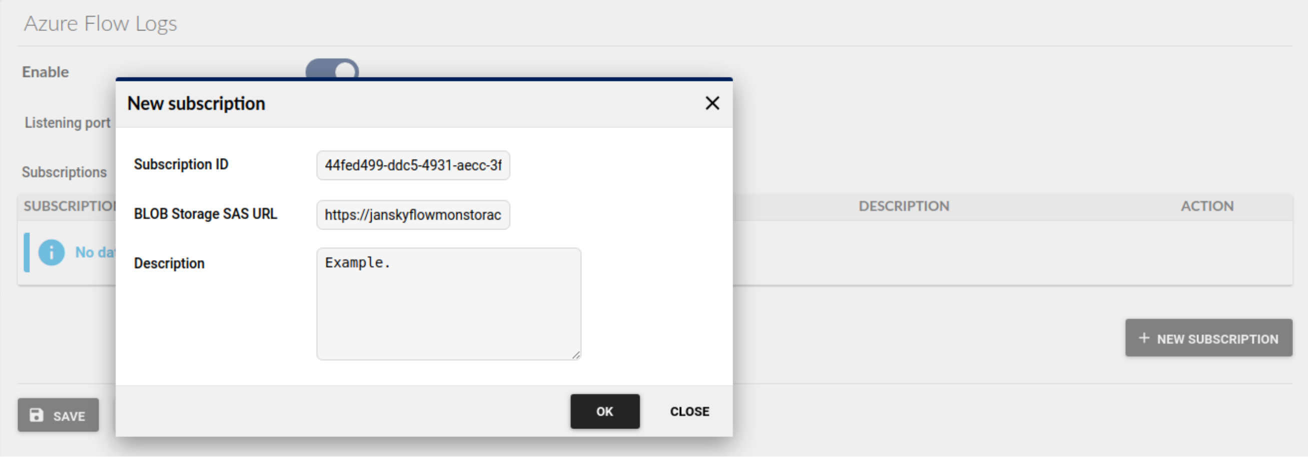
Navigate to: **Configuration Center -> FMC Configuration -> Azure Flow Logs**

Toggle the **Enable** button and select the previously created **Listening port** from the drop-down menu.

Click the **New Subscription** button which allows you to configure a list of subscriptions. This list specifies which flow logs will be obtained and processed. In order for the Flowmon Collector to access the flow logs, it requires URL of **Shared Access Signature** (SAS) created for the Azure Blob Storage container where the flow logs are stored. The SAS URL can be easily obtained using *Storage Explorer*. The SAS must provide permissions to **Read** and **List** blobs.



Flow logs inside a single Azure Blob Storage container may originate from several *Azure Account Subscriptions*. Therefore, you must also specify the *Subscription ID* that determines which flow logs should be processed by Flowmon Collector. You can process flow logs from multiple *Azure Account Subscriptions* by adding another subscription in the Azure Flow Logs FMC configuration page.



Azure Flow Logs

New subscription

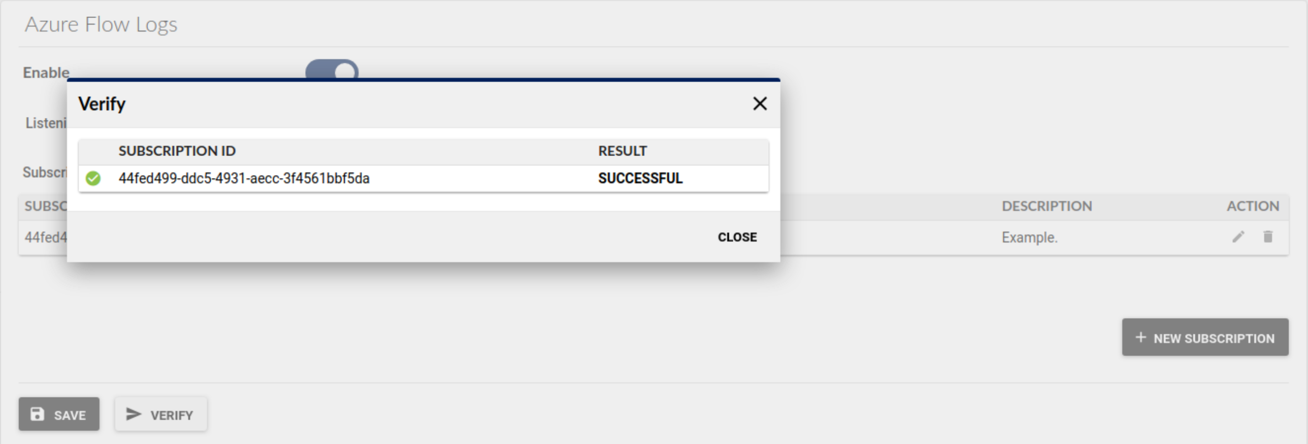
Subscription ID: 44fed499-ddc5-4931-aecc-3f

BLOB Storage SAS URL: https://janskyflowmonstorac

Description: Example.

The provided configuration can be optionally verified by clicking the **Verify** button. This will check whether Flowmon Collector is able to connect to all Azure Blob Storage containers using the provided SAS URLs and will also attempt to find the correct directory with the flow logs (using the provided subscription ID).

Note that the provided configuration undergoes the verification process every time the **Save** button is clicked.



Azure Flow Logs

Verify

SUBSCRIPTION ID	RESULT
✓ 44fed499-ddc5-4931-aecc-3f4561bbf5da	SUCCESSFUL

SUBSC	DESCRIPTION	ACTION
44fed4	Example.	

Newly created configuration must be saved (by clicking the **Save** button). This will start the process of retrieving of the flow logs. To stop the processing the flow logs, toggle the **Enable** button and click the **Save** button again. Note that your configuration is stored even when the flow log processing is disabled, so that it can be easily enabled again.

Viewing Azure NSG Flow Logs in Monitoring Center

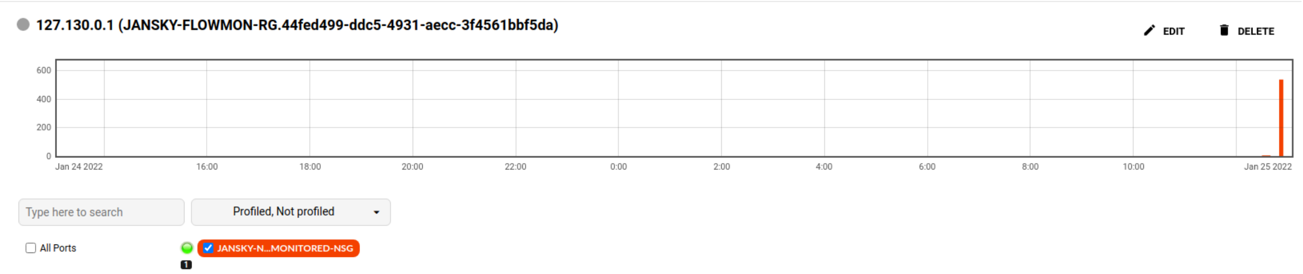
Multiple flow sources are created when using Azure NSG Flow Logs. Each flow source is internally assigned a unique IP address (from subnet 127.130.0.0/16) and corresponds to a single resource group inside in the Azure Account Subscription. The name of the source has the following format: **resource_group.subscription_id**.

All sources can be found in **Flowmon Monitoring Center -> Sources.**

Click the **Profile** button if you want to divide the flow source into separate channel. Each channel contains flows from a particular **Network Security Group** and is uniquely identified by its name.

Select all available subnets and click the **Save** button.

It is possible to view and analyze the flows from the flow logs as if they were flows from regular data sources.



127.130.0.1 (JANSKY-FLOWMON-RG.44fed499-ddc5-4931-aecc-3f4561bbf5da)

Flow Database Fields

This page contains description of fields which can be saved and displayed on Flowmon Collector.

TLS Main

All these fields are processed in protocol versions from SSL 3.0 up to TLS 1.2. For SSL 2.0 only the Server version is processed. Some fields are not processed for TLS 1.3 and above, see the "Notes" section of each field.

Content type

Description: Contains Content types of all TLS messages in a flow.
Structure: flags
Example: CCS-ALERT-HS-DATA
Filter: link
Possible values: link
Source IPFIX element: FLOWMON_TLS_CONTENT_TYPE, pen=39499, id=330
Depends on monitoring port extension: TLS main

Handshake type

Description: Every TLS Handshake message have some Handshake type value. This field contains Handshake types of all TLS Handhake messages.
Structure: flags
Example: CH-SH-CER-SHD-NST
Filter: link
Possible values: link
Source IPFIX element: FLOWMON_TLS_HANDSHAKE_TYPE, pen=39499, id=331
Depends on monitoring port extension: TLS main

Setup time

Description: Duration of TLS Handshake in miliseconds.
Structure: number of millisecond
Example: 3.123 ms
Filter: link
Source IPFIX element: FLOWMON_TLS_SETUP_TIME, pen=39499, id=332
Depends on monitoring port extension: TLS main
Notes: For protocol version TLS 1.2 and below (except SSL 2.0), the setup time is computed as the difference between ClientHello message arrival time and client (or server) ChangeCipherSpec message arrival time (the latter one).
For protocol version TLS 1.3 it is computed as the difference between ClientHello message arrival time and the arrival time of the first ApplicationData message from client after the first ApplicationData message from server was received.

Server version

Description: Version of TLS protocol used in communication. It is chosen by server and send in ServerHello message.
Structure: string or hexadecimal number
Example: TLS 1.3
Filter: link
Possible values: link
Source IPFIX element: FLOWMON_TLS_SERVER_VERSION, pen=39499, id=333
Depends on monitoring port extension: TLS main

Server random ID

Description: Value of the field called “Random” in ServerHello message.
Structure: byte array
Example: 50839c9fe3bf7e9175dce3716adb1be4c8169f24f7c4a0122cb45fdfb52fd776
Filter: link
Source IPFIX element: FLOWMON_TLS_SERVER_RANDOM, pen=39499, id=334
Depends on monitoring port extension: TLS main

Server session ID

Description: Session ID value from the ServerHello message.
Structure: byte array
Example: 98a0e4c3c67b22caf4af26022bd98b44b005dfd53b90b0a840902c47dcbe2330
Filter: link
Source IPFIX element: FLOWMON_TLS_SERVER_SESSION_ID, pen=39499, id=335
Depends on monitoring port extension: TLS main

Server cipher suite

Description: Cipher suite used in communication. It is selected by server and send in ServerHello message.
Structure: string or hexadecimal number
Example: RSA_WITH_AES_128_CBC_SHA
Filter: link

Possible values: link
Source IPFIX element: FLOWMON_TLS_CIPHER_SUITE, pen=39499, id=336
Depends on monitoring port extension: TLS main

L7 protocol negotiation

Description: Application protocol contained in the TLS session (the upper layer protocol). It is send in ALPN extenion (16) in ServerHello message.
Structure: string
Example: http/1.1
Filter: link
Possible values: https://www.iana.org/assignments/tls-extensiontype-values/tls-extensiontype-values.xhtml#alpn-protocol-ids
Source IPFIX element: FLOWMON_TLS_ALPN, pen=39499, id=337
Depends on monitoring port extension: TLS main
Notes: This field is not possible to obtain in TLS protocol version 1.3 and above because it is encrypted.

Server name (SNI)

Description: Name of the server the client is connecting to. It is send in ClientHello message in server_name extension (0).
Structure: string
Example: server.example.com
Filter: link
Source IPFIX element: FLOWMON_TLS_SNI, pen=39499, id=338
Notes: The maximal length of the string is 63 characters, longer strings are cut off from right.
Depends on monitoring port extension: TLS main

Server name length

Description: Full length of the Server name (SNI) value.
Structure: number
Example: 25
Filter: link
Source IPFIX element: FLOWMON_TLS_SNI_LENGTH, pen=39499, id=339
Depends on monitoring port extension: TLS main

TLS Client

Client version

Description: Highest (or preferred) protocol version the client offered to use in communication.
Structure: string or hexadecimal number
Example: TLS 1.3
Filter: link
Possible values: link

Source IPFIX element: FLOWMON_TLS_CLIENT_VERSION, pen=39499, id=340
Depends on monitoring port extension: TLS client
Notes: In TLS version 1.2 and below, the value is send in ClientHello message header. In TLS version 1.3 the value is send in ClientHello message in supported_versions extension (43).

Cipher suites

Description: First 8 cipher suites offered by client in ClientHello message.
Structure: list of hexadecimal numbers
Example: 0x12AB,0x4321,0x54AB
Filter: link
Possible values: link
Source IPFIX element: FLOWMON_TLS_CIPHER_SUITES, pen=39499, id=341
Depends on monitoring port extension: TLS client

Client random ID

Description: Value of the field called "Random" in ClientHello message.
Structure: byte array
Example: 50839c9fe3bf7e9175dce3716adb1be4c8169f24f7c4a0122cb45fdfb52fd776
Filter: link
Source IPFIX element: FLOWMON_TLS_CLIENT_RANDOM, pen=39499, id=342
Depends on monitoring port extension: TLS client

Client session ID

Description: Session ID value from the ClientHello message.
Structure: byte array
Example: 98a0e4c3c67b22caf4af26022bd98b44b005dfd53b90b0a840902c47dcbe2330
Filter: link
Source IPFIX element: FLOWMON_TLS_CLIENT_SESSION_ID, pen=39499, id=343
Depends on monitoring port extension: TLS client

Extension types

Description: First 28 extension types send in ClientHello message.
Structure: list of numbers
Example: 0,43,11
Filter: link
Possible values: https://www.iana.org/assignments/tls-extensiontype-values/tls-extensiontype-values.xhtml
Source IPFIX element: FLOWMON_TLS_EXTENSION_TYPES, pen=39499, id=344
Depends on monitoring port extension: TLS client

Extension lengths

Description: First 28 lengths of extensions send in ClientHello message.
Structure: list of numbers
Example: 124,53,25

Filter: link
Source IPFIX element: FLOWMON_TLS_EXTENSION_LENGTHS, pen=39499, id=345
Depends on monitoring port extension: TLS client

Elliptic curves

Description: First 8 elliptic curves offered in ClientHello message in supported_groups extension (10)
Structure: list of strings or hexadecimal numbers
Example: x25519,secp224k1,ffdhe2048
Filter: link
Possible values: https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-8
Source IPFIX element: FLOWMON_TLS_ELLIPTIC_CURVES, pen=39499, id=346
Depends on monitoring port extension: TLS client

Elliptic curve point formats

Description: Elliptic curve point formats offerd in ClientHello message in ec_point_formats extension (11).
Structure: list of strings or numbers
Example: uncompressed,ansiX962_compressed_prime
Filter: link
Possible values: link
Source IPFIX element: FLOWMON_TLS_EC_POINT_FORMATS, pen=39499, 347
Depends on monitoring port extension: TLS client

Client key length

Description: Length of the client's public key used during Key Exchange phase.
Structure: number of bits
Example: 256
Filter: link
Source IPFIX element: FLOWMON_TLS_CLIENT_KEY_LENGTH, pen=39499, id=348
Depends on monitoring port extension: TLS client
Notes: In TLS version 1.2 and below, it is the length of the public key structure send in ClientKeyExchange handshake message.
In TLS 1.3 it is the length of the chosen key exchange structure taken from key_share extension (51).

TLS Certificate

The following fields are being taken from the first certificate send by server in Certificate message. It is not possible to obtain these fields in TLS protocol version 1.3 and above because they are encrypted.

Issuer common name

Description: Common name of the certificate's issuer.
Structure: string

Example: Google Internet Authority G3
Filter: link
Source IPFIX element: FLOWMON_TLS_ISSUER_CN, pen=39499, id=349
Depends on monitoring port extension: TLS certificate

Subject common name

Description: Common name of the certificate's subject.
Structure: string
Example: server.example.com
Filter: link
Source IPFIX element: FLOWMON_TLS_SUBJECT_CN, pen=39499, id=350
Depends on monitoring port extension: TLS certificate

Subject organization name

Description: Organization name of the certificate's subject.
Structure: string
Example: Example Organization
Filter: link
Source IPFIX element: FLOWMON_TLS_SUBJECT_ON, pen=39499, id=351
Depends on monitoring port extension: TLS certificate

Certificate validity from

Description: Date and time from which the certificate is valid.
Structure: timestamp
Example: 2018-09-13 10:47:00
Filter: link
Source IPFIX element: FLOWMON_TLS_VALIDITY_NOT_BEFORE, pen=39499, id=352
Depends on monitoring port extension: TLS certificate

Certificate validity to

Description: Date and time to which the certificate is valid.
Structure: timestamp
Example: 2018-09-13 10:47:00
Filter: link
Source IPFIX element: FLOWMON_TLS_VALIDITY_NOT_AFTER, pen=39499, id=353
Depends on monitoring port extension: TLS certificate

Signature algorithm

Description: Certificate's signature algorithm.
Structure: string
Example: sha512WithRSAEncryption
Filter: link
Source IPFIX element: FLOWMON_TLS_SIGNATURE_ALG, pen=39499, id=354
Depends on monitoring port extension: TLS certificate

Public key algorithm

Description: Algorithm of the certificate's public key.
Structure: string
Example: rsaEncryption
Filter: link
Source IPFIX element: FLOWMON_TLS_PUBLIC_KEY_ALG, pen=39499, id=355
Depends on monitoring port extension: TLS certificate

Public key length

Description: Length of the certificate's public key.
Structure: number of bits
Example: 256
FIlter: link
Source IPFIX element: FLOWMON_TLS_PUBLIC_KEY_LENGTH, pen=39499, id=356
Depends on monitoring port extension: TLS certificate

TLS JA3

JA3 fingerprint

Description: JA3 fingerprint of a client.
Structure: byte array
Example: 50839c9fe3bf7e9175dce3716adb1be4
Filter: link
Source IPFIX element: FLOWMON_TLS_JA3_FINGERPRINT, pen=39499, id=357
Depends on monitoring port extension: TLS certificate

Possible values

TLS Content type

0x01 CCS Change Cipher Spec
0x02 ALERT Alert
0x03 HS Handshake
0x04 DATA Application data

TLS Handshake type

0x00000001 HRQ Hello Request
0x00000002 CH Client Hello
0x00000004 SH Server Hello
0x00000008 HVER Hello Verify Request

0x00000010 NST New Session Ticket
0x00000020 EED End of Early Data
0x00000080 ENC Encrypted Extensions
0x00000100 CER Certificate
0x00000200 KSRV Server Key Exchange
0x00000400 CRQ Certificate Request
0x00000800 SHD Server Hello Done
0x00001000 CVER Certificate Verify
0x00002000 KCL Client Key Exchange
0x00004000 FIN Finished
0x00008000 CURL Certificate URL
0x00010000 CST Certificate Status
0x00020000 SUPL Supplemental Data
0x00040000 KUPD Key Update
0x00080000 MSGH Message Hash
0x80000000 UNKN Unknown

TLS Server version

0x0000, "N/A"
0x0002, "SSL 2.0"
0x0100, "DTLS 1.0 (OpenSSL pre 0.9.8f)"
0x0300, "SSL 3.0"
0x0301, "TLS 1.0"
0x0302, "TLS 1.1"
0x0303, "TLS 1.2"
0x0304, "TLS 1.3"
0x7F0E, "TLS 1.3 (draft 14)"
0x7F0F, "TLS 1.3 (draft 15)"
0x7F10, "TLS 1.3 (draft 16)"
0x7F11, "TLS 1.3 (draft 17)"
0x7F12, "TLS 1.3 (draft 18)"
0x7F13, "TLS 1.3 (draft 19)"
0x7F14, "TLS 1.3 (draft 20)"
0x7F15, "TLS 1.3 (draft 21)"
0x7F16, "TLS 1.3 (draft 22)"
0x7F17, "TLS 1.3 (draft 23)"
0x7F18, "TLS 1.3 (draft 24)"
0x7F19, "TLS 1.3 (draft 25)"
0x7F1A, "TLS 1.3 (draft 26)"
0x7F1B, "TLS 1.3 (draft 27)"
0x7F1C, "TLS 1.3 (draft 28)"
0x0A0A, "GREASE#0x0A0A"
0x1A1A, "GREASE#0x1A1A"
0x2A2A, "GREASE#0x2A2A"
0x3A3A, "GREASE#0x3A3A"
0x4A4A, "GREASE#0x4A4A"
0x5A5A, "GREASE#0x5A5A"
0x6A6A, "GREASE#0x6A6A"
0x7A7A, "GREASE#0x7A7A"
0x8A8A, "GREASE#0x8A8A"

```
0x9A9A, "GREASE#0x9A9A"
0xAAAA, "GREASE#0xAAAA"
0xBABA, "GREASE#0xBABA"
0xCACA, "GREASE#0xCACA"
0xDADA, "GREASE#0xDADA"
0xEAEA, "GREASE#0xEAEA"
0xFAFA, "GREASE#0xFAFA"
0xFB17, "TLS 1.3 (Facebook draft 23)"
0xFB1A, "TLS 1.3 (Facebook draft 26)"
0xFEFF, "DTLS 1.0"
0xFEFD, "DTLS 1.2"
```

TLS Cipher suite

```
0x0000, "N/A"
0x0001, "RSA_WITH_NULL_MD5"
0x0002, "RSA_WITH_NULL_SHA"
0x0003, "RSA_EXPORT_WITH_RC4_40_MD5"
0x0004, "RSA_WITH_RC4_128_MD5"
0x0005, "RSA_WITH_RC4_128_SHA"
0x0006, "RSA_EXPORT_WITH_RC2_CBC_40_MD5"
0x0007, "RSA_WITH_IDEA_CBC_SHA"
0x0008, "RSA_EXPORT_WITH_DES40_CBC_SHA"
0x0009, "RSA_WITH_DES_CBC_SHA"
0x000a, "RSA_WITH_3DES_EDE_CBC_SHA"
0x000b, "DH_DSS_EXPORT_WITH_DES40_CBC_SHA"
0x000c, "DH_DSS_WITH_DES_CBC_SHA"
0x000d, "DH_DSS_WITH_3DES_EDE_CBC_SHA"
0x000e, "DH_RSA_EXPORT_WITH_DES40_CBC_SHA"
0x000f, "DH_RSA_WITH_DES_CBC_SHA"
0x0010, "DH_RSA_WITH_3DES_EDE_CBC_SHA"
0x0011, "DHE_DSS_EXPORT_WITH_DES40_CBC_SHA"
0x0012, "DHE_DSS_WITH_DES_CBC_SHA"
0x0013, "DHE_DSS_WITH_3DES_EDE_CBC_SHA"
0x0014, "DHE_RSA_EXPORT_WITH_DES40_CBC_SHA"
0x0015, "DHE_RSA_WITH_DES_CBC_SHA"
0x0016, "DHE_RSA_WITH_3DES_EDE_CBC_SHA"
0x0017, "DH_anon_EXPORT_WITH_RC4_40_MD5"
0x0018, "DH_anon_WITH_RC4_128_MD5"
0x0019, "DH_anon_EXPORT_WITH_DES40_CBC_SHA"
0x001a, "DH_anon_WITH_DES_CBC_SHA"
0x001b, "DH_anon_WITH_3DES_EDE_CBC_SHA"
0x001c, "FORTEZZA_KEA_WITH_NULL_SHA"
0x001d, "FORTEZZA_KEA_WITH_FORTEZZA_CBC_SHA"
0x001E, "KRB5_WITH_DES_CBC_SHA"
0x001F, "KRB5_WITH_3DES_EDE_CBC_SHA"
0x0020, "KRB5_WITH_RC4_128_SHA"
0x0021, "KRB5_WITH_IDEA_CBC_SHA"
0x0022, "KRB5_WITH_DES_CBC_MD5"
0x0023, "KRB5_WITH_3DES_EDE_CBC_MD5"
0x0024, "KRB5_WITH_RC4_128_MD5"
```

```
0x0025, "KRB5_WITH_IDEA_CBC_MD5"
0x0026, "KRB5_EXPORT_WITH_DES_CBC_40_SHA"
0x0027, "KRB5_EXPORT_WITH_RC2_CBC_40_SHA"
0x0028, "KRB5_EXPORT_WITH_RC4_40_SHA"
0x0029, "KRB5_EXPORT_WITH_DES_CBC_40_MD5"
0x002A, "KRB5_EXPORT_WITH_RC2_CBC_40_MD5"
0x002B, "KRB5_EXPORT_WITH_RC4_40_MD5"
0x002C, "PSK_WITH_NULL_SHA"
0x002D, "DHE_PSK_WITH_NULL_SHA"
0x002E, "RSA_PSK_WITH_NULL_SHA"
0x002f, "RSA_WITH_AES_128_CBC_SHA"
0x0030, "DH_DSS_WITH_AES_128_CBC_SHA"
0x0031, "DH_RSA_WITH_AES_128_CBC_SHA"
0x0032, "DHE_DSS_WITH_AES_128_CBC_SHA"
0x0033, "DHE_RSA_WITH_AES_128_CBC_SHA"
0x0034, "DH_anon_WITH_AES_128_CBC_SHA"
0x0035, "RSA_WITH_AES_256_CBC_SHA"
0x0036, "DH_DSS_WITH_AES_256_CBC_SHA"
0x0037, "DH_RSA_WITH_AES_256_CBC_SHA"
0x0038, "DHE_DSS_WITH_AES_256_CBC_SHA"
0x0039, "DHE_RSA_WITH_AES_256_CBC_SHA"
0x003A, "DH_anon_WITH_AES_256_CBC_SHA"
0x003B, "RSA_WITH_NULL_SHA256"
0x003C, "RSA_WITH_AES_128_CBC_SHA256"
0x003D, "RSA_WITH_AES_256_CBC_SHA256"
0x003E, "DH_DSS_WITH_AES_128_CBC_SHA256"
0x003F, "DH_RSA_WITH_AES_128_CBC_SHA256"
0x0040, "DHE_DSS_WITH_AES_128_CBC_SHA256"
0x0041, "RSA_WITH_CAMELLIA_128_CBC_SHA"
0x0042, "DH_DSS_WITH_CAMELLIA_128_CBC_SHA"
0x0043, "DH_RSA_WITH_CAMELLIA_128_CBC_SHA"
0x0044, "DHE_DSS_WITH_CAMELLIA_128_CBC_SHA"
0x0045, "DHE_RSA_WITH_CAMELLIA_128_CBC_SHA"
0x0046, "DH_anon_WITH_CAMELLIA_128_CBC_SHA"
0x0047, "ECDH_ECDSA_WITH_NULL_SHA#0x0047"
0x0048, "ECDH_ECDSA_WITH_RC4_128_SHA#0x0048"
0x0049, "ECDH_ECDSA_WITH_DES_CBC_SHA#"
0x004A, "ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA#0x004A"
0x004B, "ECDH_ECDSA_WITH_AES_128_CBC_SHA#0x004B"
0x004C, "ECDH_ECDSA_WITH_AES_256_CBC_SHA#0x004C"
0x0060, "RSA_EXPORT1024_WITH_RC4_56_MD5"
0x0061, "RSA_EXPORT1024_WITH_RC2_CBC_56_MD5"
0x0062, "RSA_EXPORT1024_WITH_DES_CBC_SHA"
0x0063, "DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA"
0x0064, "RSA_EXPORT1024_WITH_RC4_56_SHA"
0x0065, "DHE_DSS_EXPORT1024_WITH_RC4_56_SHA"
0x0066, "DHE_DSS_WITH_RC4_128_SHA"
0x0067, "DHE_RSA_WITH_AES_128_CBC_SHA256"
0x0068, "DH_DSS_WITH_AES_256_CBC_SHA256"
0x0069, "DH_RSA_WITH_AES_256_CBC_SHA256"
0x006A, "DHE_DSS_WITH_AES_256_CBC_SHA256"
```

```
0x006B, "DHE_RSA_WITH_AES_256_CBC_SHA256"
0x006C, "DH_anon_WITH_AES_128_CBC_SHA256"
0x006D, "DH_anon_WITH_AES_256_CBC_SHA256"
0x0080, "GOSTR341094_WITH_28147_CNT_IMIT"
0x0081, "GOSTR341001_WITH_28147_CNT_IMIT"
0x0082, "GOSTR341094_WITH_NULL_GOSTR3411"
0x0083, "GOSTR341001_WITH_NULL_GOSTR3411"
0x0084, "RSA_WITH_CAMELLIA_256_CBC_SHA"
0x0085, "DH_DSS_WITH_CAMELLIA_256_CBC_SHA"
0x0086, "DH_RSA_WITH_CAMELLIA_256_CBC_SHA"
0x0087, "DHE_DSS_WITH_CAMELLIA_256_CBC_SHA"
0x0088, "DHE_RSA_WITH_CAMELLIA_256_CBC_SHA"
0x0089, "DH_anon_WITH_CAMELLIA_256_CBC_SHA"
0x008A, "PSK_WITH_RC4_128_SHA"
0x008B, "PSK_WITH_3DES_EDE_CBC_SHA"
0x008C, "PSK_WITH_AES_128_CBC_SHA"
0x008D, "PSK_WITH_AES_256_CBC_SHA"
0x008E, "DHE_PSK_WITH_RC4_128_SHA"
0x008F, "DHE_PSK_WITH_3DES_EDE_CBC_SHA"
0x0090, "DHE_PSK_WITH_AES_128_CBC_SHA"
0x0091, "DHE_PSK_WITH_AES_256_CBC_SHA"
0x0092, "RSA_PSK_WITH_RC4_128_SHA"
0x0093, "RSA_PSK_WITH_3DES_EDE_CBC_SHA"
0x0094, "RSA_PSK_WITH_AES_128_CBC_SHA"
0x0095, "RSA_PSK_WITH_AES_256_CBC_SHA"
0x0096, "RSA_WITH_SEED_CBC_SHA"
0x0097, "DH_DSS_WITH_SEED_CBC_SHA"
0x0098, "DH_RSA_WITH_SEED_CBC_SHA"
0x0099, "DHE_DSS_WITH_SEED_CBC_SHA"
0x009A, "DHE_RSA_WITH_SEED_CBC_SHA"
0x009B, "DH_anon_WITH_SEED_CBC_SHA"
0x009C, "RSA_WITH_AES_128_GCM_SHA256"
0x009D, "RSA_WITH_AES_256_GCM_SHA384"
0x009E, "DHE_RSA_WITH_AES_128_GCM_SHA256"
0x009F, "DHE_RSA_WITH_AES_256_GCM_SHA384"
0x00A0, "DH_RSA_WITH_AES_128_GCM_SHA256"
0x00A1, "DH_RSA_WITH_AES_256_GCM_SHA384"
0x00A2, "DHE_DSS_WITH_AES_128_GCM_SHA256"
0x00A3, "DHE_DSS_WITH_AES_256_GCM_SHA384"
0x00A4, "DH_DSS_WITH_AES_128_GCM_SHA256"
0x00A5, "DH_DSS_WITH_AES_256_GCM_SHA384"
0x00A6, "DH_anon_WITH_AES_128_GCM_SHA256"
0x00A7, "DH_anon_WITH_AES_256_GCM_SHA384"
0x00A8, "PSK_WITH_AES_128_GCM_SHA256"
0x00A9, "PSK_WITH_AES_256_GCM_SHA384"
0x00AA, "DHE_PSK_WITH_AES_128_GCM_SHA256"
0x00AB, "DHE_PSK_WITH_AES_256_GCM_SHA384"
0x00AC, "RSA_PSK_WITH_AES_128_GCM_SHA256"
0x00AD, "RSA_PSK_WITH_AES_256_GCM_SHA384"
0x00AE, "PSK_WITH_AES_128_CBC_SHA256"
0x00AF, "PSK_WITH_AES_256_CBC_SHA384"
```

```
0x00B0, "PSK_WITH_NULL_SHA256"
0x00B1, "PSK_WITH_NULL_SHA384"
0x00B2, "DHE_PSK_WITH_AES_128_CBC_SHA256"
0x00B3, "DHE_PSK_WITH_AES_256_CBC_SHA384"
0x00B4, "DHE_PSK_WITH_NULL_SHA256"
0x00B5, "DHE_PSK_WITH_NULL_SHA384"
0x00B6, "RSA_PSK_WITH_AES_128_CBC_SHA256"
0x00B7, "RSA_PSK_WITH_AES_256_CBC_SHA384"
0x00B8, "RSA_PSK_WITH_NULL_SHA256"
0x00B9, "RSA_PSK_WITH_NULL_SHA384"
0x00BA, "RSA_WITH_CAMELLIA_128_CBC_SHA256"
0x00BB, "DH_DSS_WITH_CAMELLIA_128_CBC_SHA256"
0x00BC, "DH_RSA_WITH_CAMELLIA_128_CBC_SHA256"
0x00BD, "DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256"
0x00BE, "DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256"
0x00BF, "DH_anon_WITH_CAMELLIA_128_CBC_SHA256"
0x00C0, "RSA_WITH_CAMELLIA_256_CBC_SHA256"
0x00C1, "DH_DSS_WITH_CAMELLIA_256_CBC_SHA256"
0x00C2, "DH_RSA_WITH_CAMELLIA_256_CBC_SHA256"
0x00C3, "DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256"
0x00C4, "DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256"
0x00C5, "DH_anon_WITH_CAMELLIA_256_CBC_SHA256"
0x00FF, "EMPTY_RENEGOTIATION_INFO_SCSV"
0x0A0A, "Reserved (GREASE)#0x0A0A"
0x1301, "AES_128_GCM_SHA256"
0x1302, "AES_256_GCM_SHA384"
0x1303, "CHACHA20_POLY1305_SHA256"
0x1304, "AES_128_CCM_SHA256"
0x1305, "AES_128_CCM_8_SHA256"
0x1A1A, "Reserved (GREASE)#0x1A1A"
0x2A2A, "Reserved (GREASE)#0x2A2A"
0x3A3A, "Reserved (GREASE)#0x3A3A"
0x4A4A, "Reserved (GREASE)#0x4A4A"
0x5600, "FALLBACK_SCSV"
0x5A5A, "Reserved (GREASE)#0x5A5A"
0x6A6A, "Reserved (GREASE)#0x6A6A"
0x7A7A, "Reserved (GREASE)#0x7A7A"
0x8A8A, "Reserved (GREASE)#0x8A8A"
0x9A9A, "Reserved (GREASE)#0x9A9A"
0xAAAA, "Reserved (GREASE)#0xAAAA"
0xBABA, "Reserved (GREASE)#0xBABA"
0xc001, "ECDH_ECDSA_WITH_NULL_SHA#0xC001"
0xc002, "ECDH_ECDSA_WITH_RC4_128_SHA#0xC002"
0xc003, "ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA#0xC003"
0xc004, "ECDH_ECDSA_WITH_AES_128_CBC_SHA#0xC004"
0xc005, "ECDH_ECDSA_WITH_AES_256_CBC_SHA#0xC005"
0xc006, "ECDHE_ECDSA_WITH_NULL_SHA"
0xc007, "ECDHE_ECDSA_WITH_RC4_128_SHA"
0xc008, "ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA"
0xc009, "ECDHE_ECDSA_WITH_AES_128_CBC_SHA"
0xc00a, "ECDHE_ECDSA_WITH_AES_256_CBC_SHA"
```

```
0xc00b, "ECDH_RSA_WITH_NULL_SHA"
0xc00c, "ECDH_RSA_WITH_RC4_128_SHA"
0xc00d, "ECDH_RSA_WITH_3DES_EDE_CBC_SHA"
0xc00e, "ECDH_RSA_WITH_AES_128_CBC_SHA"
0xc00f, "ECDH_RSA_WITH_AES_256_CBC_SHA"
0xc010, "ECDHE_RSA_WITH_NULL_SHA"
0xc011, "ECDHE_RSA_WITH_RC4_128_SHA"
0xc012, "ECDHE_RSA_WITH_3DES_EDE_CBC_SHA"
0xc013, "ECDHE_RSA_WITH_AES_128_CBC_SHA"
0xc014, "ECDHE_RSA_WITH_AES_256_CBC_SHA"
0xc015, "ECDH_anon_WITH_NULL_SHA"
0xc016, "ECDH_anon_WITH_RC4_128_SHA"
0xc017, "ECDH_anon_WITH_3DES_EDE_CBC_SHA"
0xc018, "ECDH_anon_WITH_AES_128_CBC_SHA"
0xc019, "ECDH_anon_WITH_AES_256_CBC_SHA"
0xC01A, "SRP_SHA_WITH_3DES_EDE_CBC_SHA"
0xC01B, "SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA"
0xC01C, "SRP_SHA_DSS_WITH_3DES_EDE_CBC_SHA"
0xC01D, "SRP_SHA_WITH_AES_128_CBC_SHA"
0xC01E, "SRP_SHA_RSA_WITH_AES_128_CBC_SHA"
0xC01F, "SRP_SHA_DSS_WITH_AES_128_CBC_SHA"
0xC020, "SRP_SHA_WITH_AES_256_CBC_SHA"
0xC021, "SRP_SHA_RSA_WITH_AES_256_CBC_SHA"
0xC022, "SRP_SHA_DSS_WITH_AES_256_CBC_SHA"
0xC023, "ECDHE_ECDSA_WITH_AES_128_CBC_SHA256"
0xC024, "ECDHE_ECDSA_WITH_AES_256_CBC_SHA384"
0xC025, "ECDH_ECDSA_WITH_AES_128_CBC_SHA256"
0xC026, "ECDH_ECDSA_WITH_AES_256_CBC_SHA384"
0xC027, "ECDHE_RSA_WITH_AES_128_CBC_SHA256"
0xC028, "ECDHE_RSA_WITH_AES_256_CBC_SHA384"
0xC029, "ECDH_RSA_WITH_AES_128_CBC_SHA256"
0xC02A, "ECDH_RSA_WITH_AES_256_CBC_SHA384"
0xC02B, "ECDHE_ECDSA_WITH_AES_128_GCM_SHA256"
0xC02C, "ECDHE_ECDSA_WITH_AES_256_GCM_SHA384"
0xC02D, "ECDH_ECDSA_WITH_AES_128_GCM_SHA256"
0xC02E, "ECDH_ECDSA_WITH_AES_256_GCM_SHA384"
0xC02F, "ECDHE_RSA_WITH_AES_128_GCM_SHA256"
0xC030, "ECDHE_RSA_WITH_AES_256_GCM_SHA384"
0xC031, "ECDH_RSA_WITH_AES_128_GCM_SHA256"
0xC032, "ECDH_RSA_WITH_AES_256_GCM_SHA384"
0xC033, "ECDHE_PSK_WITH_RC4_128_SHA"
0xC034, "ECDHE_PSK_WITH_3DES_EDE_CBC_SHA"
0xC035, "ECDHE_PSK_WITH_AES_128_CBC_SHA"
0xC036, "ECDHE_PSK_WITH_AES_256_CBC_SHA"
0xC037, "ECDHE_PSK_WITH_AES_128_CBC_SHA256"
0xC038, "ECDHE_PSK_WITH_AES_256_CBC_SHA384"
0xC039, "ECDHE_PSK_WITH_NULL_SHA"
0xC03A, "ECDHE_PSK_WITH_NULL_SHA256"
0xC03B, "ECDHE_PSK_WITH_NULL_SHA384"
0xC03C, "RSA_WITH_ARIA_128_CBC_SHA256"
0xC03D, "RSA_WITH_ARIA_256_CBC_SHA384"
```

```
0xC03E, "DH_DSS_WITH_ARIA_128_CBC_SHA256"
0xC03F, "DH_DSS_WITH_ARIA_256_CBC_SHA384"
0xC040, "DH_RSA_WITH_ARIA_128_CBC_SHA256"
0xC041, "DH_RSA_WITH_ARIA_256_CBC_SHA384"
0xC042, "DHE_DSS_WITH_ARIA_128_CBC_SHA256"
0xC043, "DHE_DSS_WITH_ARIA_256_CBC_SHA384"
0xC044, "DHE_RSA_WITH_ARIA_128_CBC_SHA256"
0xC045, "DHE_RSA_WITH_ARIA_256_CBC_SHA384"
0xC046, "DH_anon_WITH_ARIA_128_CBC_SHA256"
0xC047, "DH_anon_WITH_ARIA_256_CBC_SHA384"
0xC048, "ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256"
0xC049, "ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384"
0xC04A, "ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256"
0xC04B, "ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384"
0xC04C, "ECDHE_RSA_WITH_ARIA_128_CBC_SHA256"
0xC04D, "ECDHE_RSA_WITH_ARIA_256_CBC_SHA384"
0xC04E, "ECDH_RSA_WITH_ARIA_128_CBC_SHA256"
0xC04F, "ECDH_RSA_WITH_ARIA_256_CBC_SHA384"
0xC050, "RSA_WITH_ARIA_128_GCM_SHA256"
0xC051, "RSA_WITH_ARIA_256_GCM_SHA384"
0xC052, "DHE_RSA_WITH_ARIA_128_GCM_SHA256"
0xC053, "DHE_RSA_WITH_ARIA_256_GCM_SHA384"
0xC054, "DH_RSA_WITH_ARIA_128_GCM_SHA256"
0xC055, "DH_RSA_WITH_ARIA_256_GCM_SHA384"
0xC056, "DHE_DSS_WITH_ARIA_128_GCM_SHA256"
0xC057, "DHE_DSS_WITH_ARIA_256_GCM_SHA384"
0xC058, "DH_DSS_WITH_ARIA_128_GCM_SHA256"
0xC059, "DH_DSS_WITH_ARIA_256_GCM_SHA384"
0xC05A, "DH_anon_WITH_ARIA_128_GCM_SHA256"
0xC05B, "DH_anon_WITH_ARIA_256_GCM_SHA384"
0xC05C, "ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256"
0xC05D, "ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384"
0xC05E, "ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256"
0xC05F, "ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384"
0xC060, "ECDHE_RSA_WITH_ARIA_128_GCM_SHA256"
0xC061, "ECDHE_RSA_WITH_ARIA_256_GCM_SHA384"
0xC062, "ECDH_RSA_WITH_ARIA_128_GCM_SHA256"
0xC063, "ECDH_RSA_WITH_ARIA_256_GCM_SHA384"
0xC064, "PSK_WITH_ARIA_128_CBC_SHA256"
0xC065, "PSK_WITH_ARIA_256_CBC_SHA384"
0xC066, "DHE_PSK_WITH_ARIA_128_CBC_SHA256"
0xC067, "DHE_PSK_WITH_ARIA_256_CBC_SHA384"
0xC068, "RSA_PSK_WITH_ARIA_128_CBC_SHA256"
0xC069, "RSA_PSK_WITH_ARIA_256_CBC_SHA384"
0xC06A, "PSK_WITH_ARIA_128_GCM_SHA256"
0xC06B, "PSK_WITH_ARIA_256_GCM_SHA384"
0xC06C, "DHE_PSK_WITH_ARIA_128_GCM_SHA256"
0xC06D, "DHE_PSK_WITH_ARIA_256_GCM_SHA384"
0xC06E, "RSA_PSK_WITH_ARIA_128_GCM_SHA256"
0xC06F, "RSA_PSK_WITH_ARIA_256_GCM_SHA384"
0xC070, "ECDHE_PSK_WITH_ARIA_128_CBC_SHA256"
```

```
0xC071, "ECDHE_PSK_WITH_ARIA_256_CBC_SHA384"
0xC072, "ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256"
0xC073, "ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384"
0xC074, "ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256"
0xC075, "ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384"
0xC076, "ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256"
0xC077, "ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384"
0xC078, "ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256"
0xC079, "ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384"
0xC07A, "RSA_WITH_CAMELLIA_128_GCM_SHA256"
0xC07B, "RSA_WITH_CAMELLIA_256_GCM_SHA384"
0xC07C, "DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256"
0xC07D, "DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384"
0xC07E, "DH_RSA_WITH_CAMELLIA_128_GCM_SHA256"
0xC07F, "DH_RSA_WITH_CAMELLIA_256_GCM_SHA384"
0xC080, "DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256"
0xC081, "DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384"
0xC082, "DH_DSS_WITH_CAMELLIA_128_GCM_SHA256"
0xC083, "DH_DSS_WITH_CAMELLIA_256_GCM_SHA384"
0xC084, "DH_anon_WITH_CAMELLIA_128_GCM_SHA256"
0xC085, "DH_anon_WITH_CAMELLIA_256_GCM_SHA384"
0xC086, "ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256"
0xC087, "ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384"
0xC088, "ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256"
0xC089, "ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384"
0xC08A, "ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256"
0xC08B, "ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384"
0xC08C, "ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256"
0xC08D, "ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384"
0xC08E, "PSK_WITH_CAMELLIA_128_GCM_SHA256"
0xC08F, "PSK_WITH_CAMELLIA_256_GCM_SHA384"
0xC090, "DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256"
0xC091, "DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384"
0xC092, "RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256"
0xC093, "RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384"
0xC094, "PSK_WITH_CAMELLIA_128_CBC_SHA256"
0xC095, "PSK_WITH_CAMELLIA_256_CBC_SHA384"
0xC096, "DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256"
0xC097, "DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384"
0xC098, "RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256"
0xC099, "RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384"
0xC09A, "ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256"
0xC09B, "ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384"
0xC09C, "RSA_WITH_AES_128_CCM"
0xC09D, "RSA_WITH_AES_256_CCM"
0xC09E, "DHE_RSA_WITH_AES_128_CCM"
0xC09F, "DHE_RSA_WITH_AES_256_CCM"
0xC0A0, "RSA_WITH_AES_128_CCM_8"
0xC0A1, "RSA_WITH_AES_256_CCM_8"
0xC0A2, "DHE_RSA_WITH_AES_128_CCM_8"
0xC0A3, "DHE_RSA_WITH_AES_256_CCM_8"
```

0xC0A4, "PSK_WITH_AES_128_CCM"
0xC0A5, "PSK_WITH_AES_256_CCM"
0xC0A6, "DHE_PSK_WITH_AES_128_CCM"
0xC0A7, "DHE_PSK_WITH_AES_256_CCM"
0xC0A8, "PSK_WITH_AES_128_CCM_8"
0xC0A9, "PSK_WITH_AES_256_CCM_8"
0xC0AA, "PSK_DHE_WITH_AES_128_CCM_8"
0xC0AB, "PSK_DHE_WITH_AES_256_CCM_8"
0xC0AC, "ECDHE_ECDSA_WITH_AES_128_CCM"
0xC0AD, "ECDHE_ECDSA_WITH_AES_256_CCM"
0xC0AE, "ECDHE_ECDSA_WITH_AES_128_CCM_8"
0xC0AF, "ECDHE_ECDSA_WITH_AES_256_CCM_8"
0xC0FF, "ECJPAKE_WITH_AES_128_CCM_8"
0xC100, "GOSTR341112_256_WITH_KUZNYECHIK_CTR_OMAC"
0xC101, "GOSTR341112_256_WITH_MAGMA_CTR_OMAC"
0xC102, "GOSTR341112_256_WITH_28147_CNT_IMIT"
0xCACA, "Reserved (GREASE)#0xCACA"

TLS Client version

This field has the same values as TLS Server version.

TLS Cipher suites

This field has the same values as TLS Cipher suite.

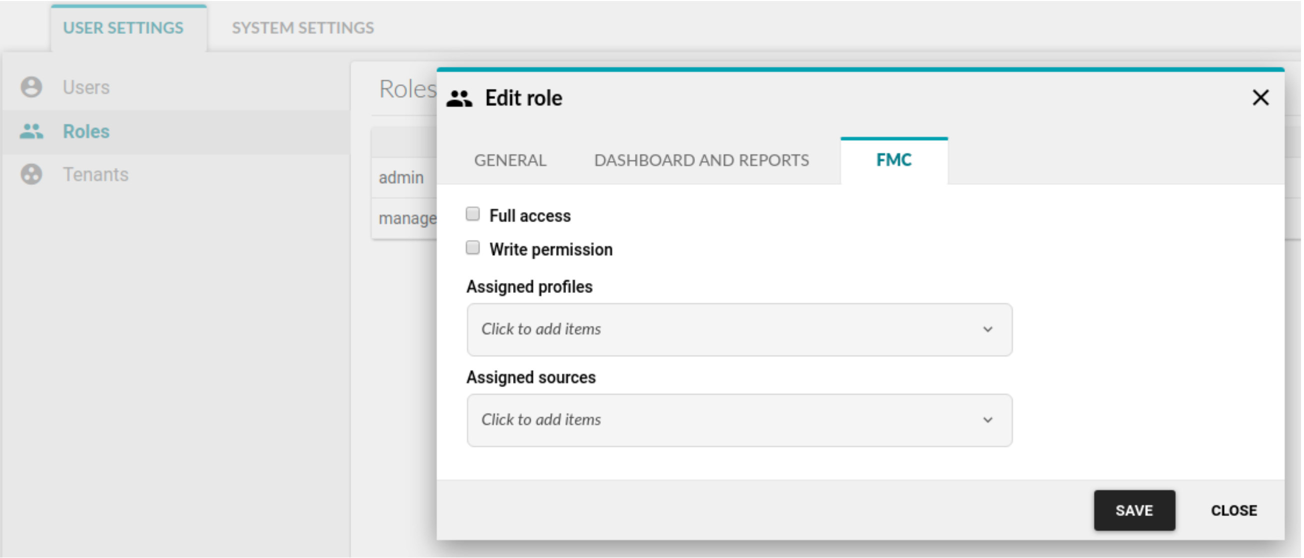
TLS Elliptic curve point formats

0, "uncompressed"
1, "ansiX962_compressed_prime"
2, "ansiX962_compressed_char2"

Role Access Permissions

For FMC module, access permissions to profiles and flow sources can be defined as well as write permissions for all settings in FMC. The permission configuration is done in Configuration Center - User Settings / Roles (see below) - more information can be found in chapter User and Roles Settings.

The access permissions are configured for roles. If the option **Full access** is checked, then the user with this role has full access to all profiles in FMC (including all channels in profile All Sources) and modify all settings. If the Full access role is not checked, the option **Write permission** can be selected. This option allows user to modify settings in FMC and edit available profiles.



If the role does not have a Full access permission, it is necessary to assign so called **root profiles** to it. The root profile is any profile which is a direct child profile (subprofile) of profile All Sources, is not a shadow profile and is of type Continuous (i.e. it is o Real continuous profile) - please see chapter Profiles. User with this role will gain access to data of assigned root profiles and the whole subtree of their subprofiles. But this user can not modify a root profile settings. You can understand root profiles as entities delimiting data which the user can access. If this user creates a new subprofile of a root profile, this subprofile can be automatically accessed by all user with access to this root profile including permission to modify it (if their role has write permission assigned - please see below).

The role can be assigned with access permissions to any flow sources (see chapter Sources). These sources will be shown on page Sources, in profile All Sources and if they are of type profiled source, then they will be included in profile group Sources. These sources can be used for definition of profile channel or report chapter.

The FMC permissions are aggregated in case more roles are assigned for one user.

Sources

This page manages all flow sources, which sent at least one flow packet to Monitoring Center. These sources are automatically added at the moment of first flow packet reception. If an SNMP info check is allowed, then the information about its name, network interfaces, their speed and status will be automatically read from each source. This information is updated every hour. If a device has enough resources, then a new profile is created in group Sources using this information (the so called **profiled source** is created). This profile can contain channels for limited number of network interface on this source (so called **profiled interfaces**). New source is also added to the "All Sources" profile. For each source, the live check operation can be enabled. This operation checks every 5 minutes whether the flow source is responding.

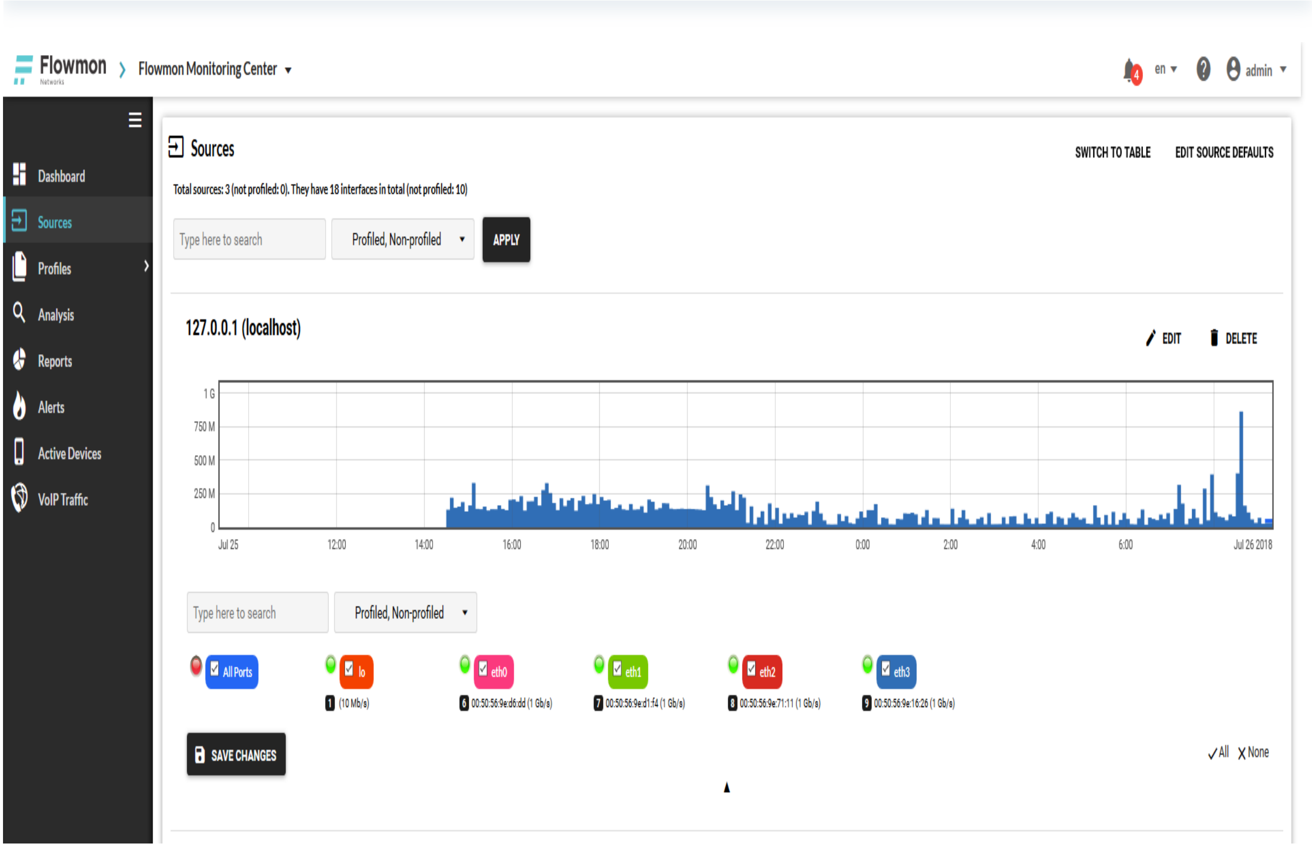
Info

Sources' visibilities can be managed within the tenant. For more information please see Tenants.

Sources can be displayed in two modes - in the panel mode and table mode. The panel mode shows only the profiled sources and each source panel contains a traffic graph and list of network interfaces obtained by SNMP (the list of interfaces is hidden by default and can be shown be clicking on a small triangle icon at the bottom of each panel). You can switch the interface into profiled state by ticking the checkbox of this interface and clicking the **Save changes** button. This creates a new channel for this interface. You can perform a search using a text field and a drop-down menu above the interface list. By clicking on **Edit** link you can change the SNMP parameters for reading the status of this source. By clicking the **Delete** link, the source is deleted. If there are still new flow packets coming from this source, the source will be added again at the moment of FMC or device restart. You can rename interface name by right-clicking on its name.

Warning

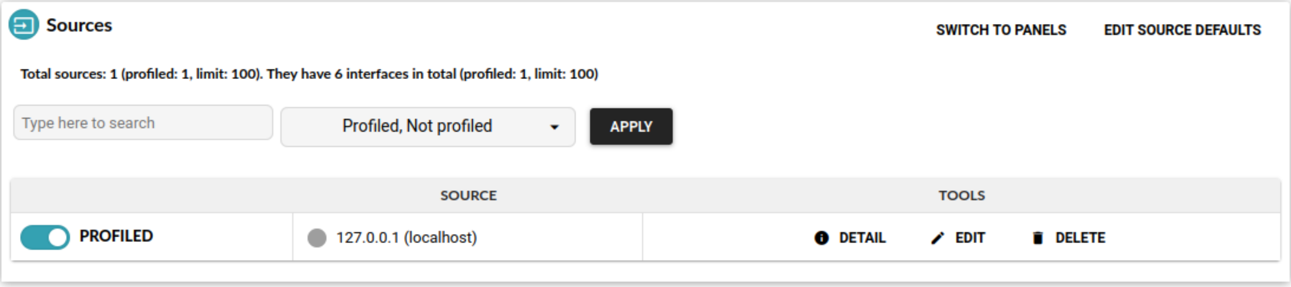
If you turn a channel or profile into non-profiled mode, its graph will be discarded and will not be recovered when turned back into profiled mode.



Total sources: 3 (not profiled: 0). They have 18 interfaces in total (not profiled: 10)

The Sources page

The table mode view (see picture below) is useful in case of having a large number of flow sources. Clicking the **Detail** button opens a form with the same content as in panel mode view. In table view you can switch the source into non-profiled mode by unchecking the **allowed/stopped** toggle switch (in case of profiled source) in status column to read "stopped". In case of enough resources, you can turn a non-profiled source to a profiled one by switching the toggle to "allowed". The **Edit** and **Delete** buttons have the same function as in the panel mode.



Sources

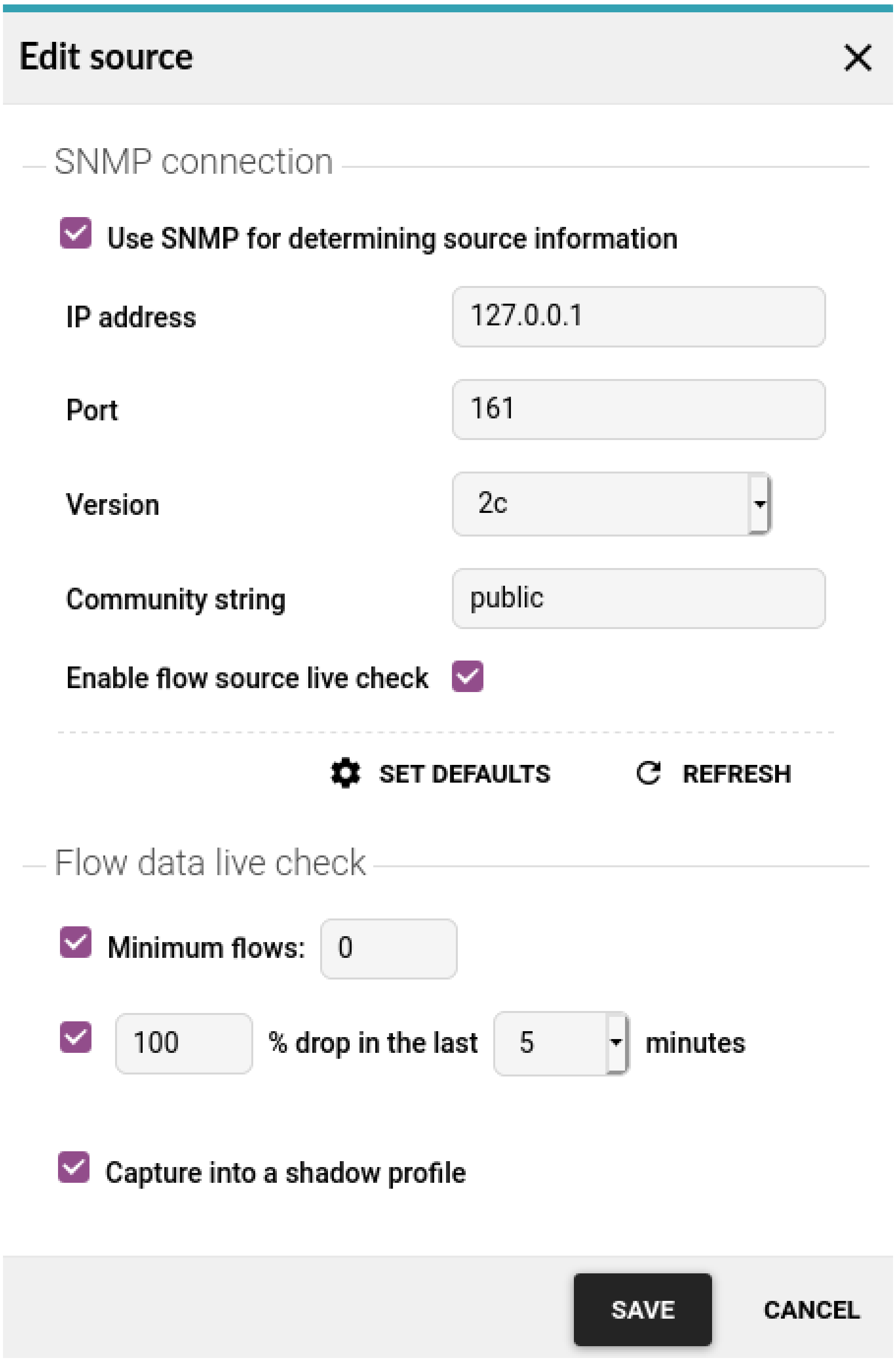
SWITCH TO PANELS EDIT SOURCE DEFAULTS

Total sources: 1 (profiled: 1, limit: 100). They have 6 interfaces in total (profiled: 1, limit: 100)

Type here to search | Profiled, Not profiled | APPLY

	SOURCE	TOOLS
PROFILED	127.0.0.1 (localhost)	DETAIL EDIT DELETE

The Sources page



Edit source

SNMP connection

☑ Use SNMP for determining source information

IP address: 127.0.0.1

Port: 161

Version: 2c

Community string: public

Enable flow source live check ☑

SET DEFAULTS REFRESH

Flow data live check

☑ Minimum flows: 0

☑ 100 % drop in the last 5 minutes

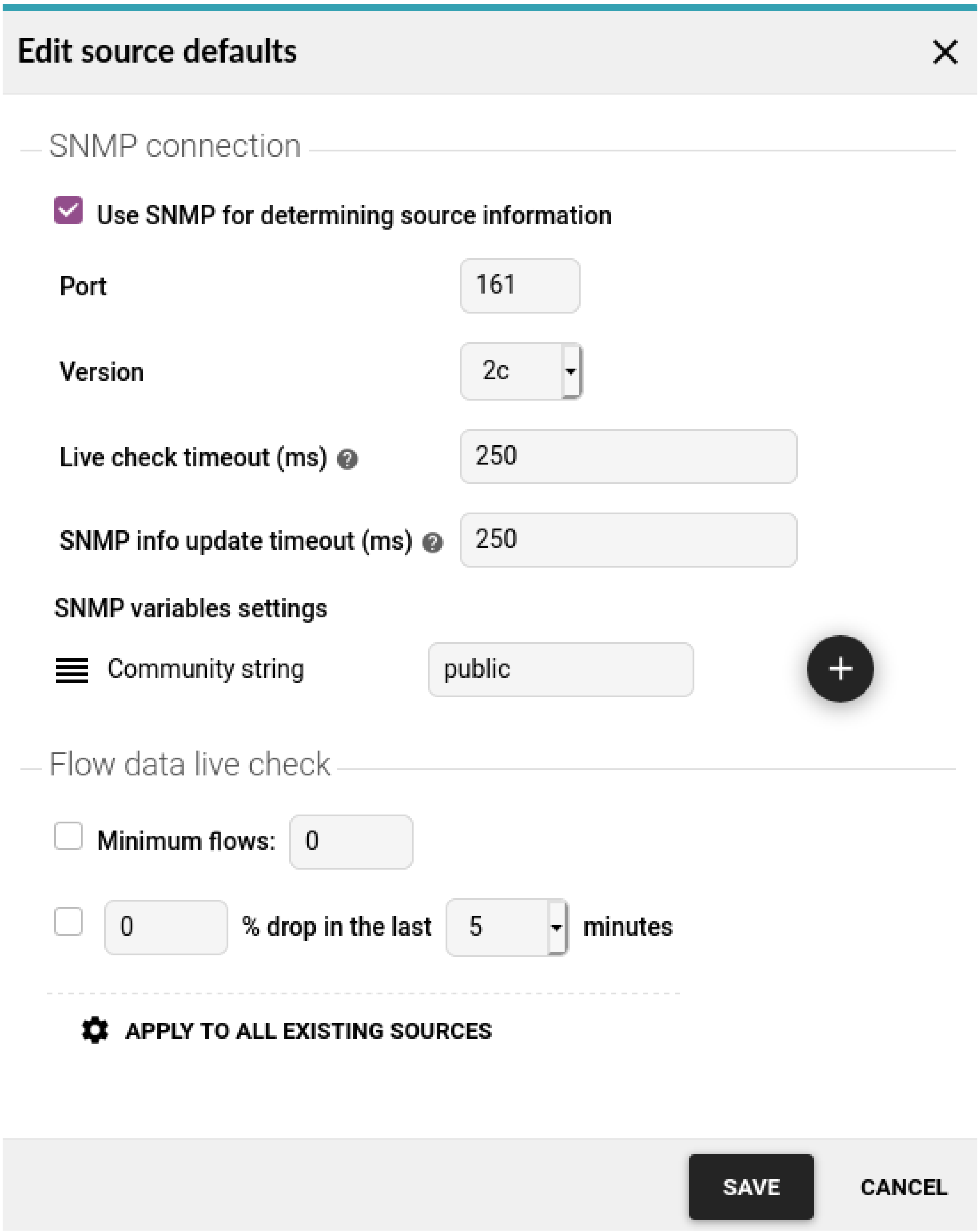
☑ Capture into a shadow profile

SAVE CANCEL

The total number of profiled or non-profiled sources and their interfaces is shown in the page header. The limit of the number of sources or interfaces can be configured in Configuration Center (see chapter Built-in Collector - Sources settings). If the source has no profiled interface incl. AllPorts, it will be turned into non-profiled mode.

If a new source is detected and the limit is not reached, the new source will be added as a profiled source and the AllPorts channel will be configured as a profiled channel. Also, an info message is shown in status icon. The AllPorts channel includes traffic from all interfaces. Selected source interfaces can be manually configured to the profiled state.

Information about the source is read automatically by the SNMP protocol (if enabled). The predefined settings are used when source is first used. The settings can be changed by clicking the **Edit source defaults** button. In dialog box, the SNMP connection can be enabled and the connection parameters can be set. It is possible to configure one or more default community strings. When a new source is detected, the system is trying the provided community strings in configured order until it is successfully connected. The right community string is then stored for this source and used again for next connection. If none of the community strings is correct, then the connection is not successful. If SNMP data have not been obtained (because of error or because this function was disabled by user), a channel AllPorts is created only.



Edit source defaults ✕

SNMP connection

☑ Use SNMP for determining source information

Port	161
Version	2c
Live check timeout (ms)	250
SNMP info update timeout (ms)	250

SNMP variables settings

Community string: public

Flow data live check

□ Minimum flows: 0

□ 0 % drop in the last 5 minutes

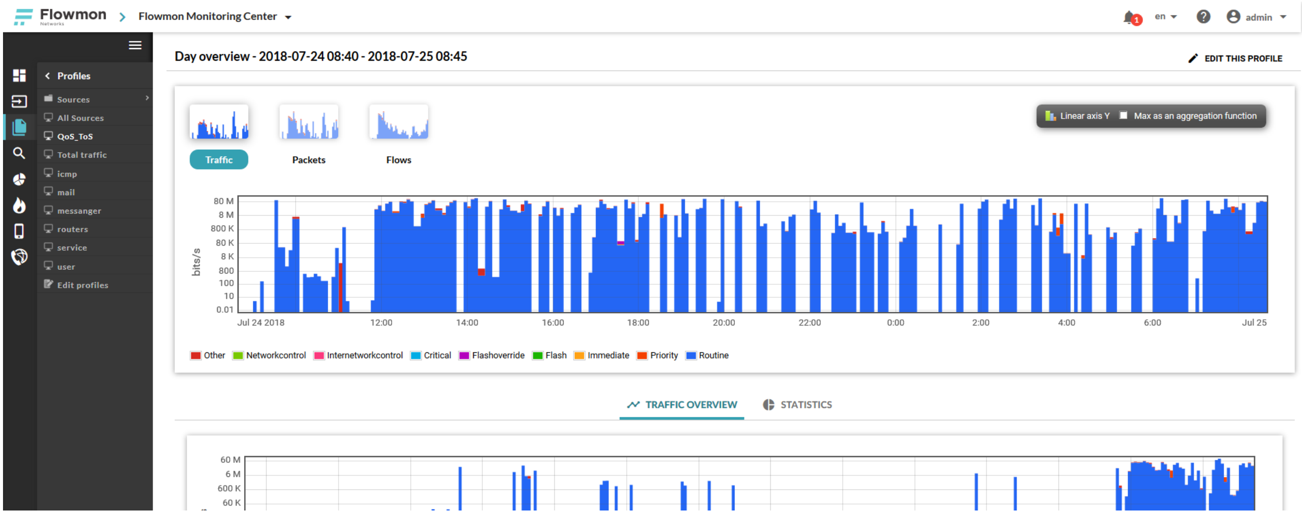
The information about source is refreshed in regular manner. The parameters of SNMP connection can be set here. If the option **Use SNMP for determining the source information** is enabled, the function **Enable flow source live check** can be enabled as well. This function tries every 5 minutes to read by SNMP a hostname of the source and if it is unsuccessful, it is reported to user into a status icon (which may lead to sending an email, syslog or SNMP trap depending on configuration). A similar check **Flow data live check** can by enabled on a source and it is checking the number of incoming flows to ensure that configured criteria is met. There is a possibility to enable two conditions each being evaluated independently. The first one **Minimum flows** compares the number of flows in last the 5 minutes interval to the defined limit. The second condition **% drop** evaluates a percentage drop in the number of flows in the last 5, 10 or 15 minutes and is evaluated every 5 minutes. If any of the enabled conditions is not met, this fact is reported into a status icon, possibly triggering other actions listed in the SNMP live check description.

Profiles

Info

Profiles' visibilities can be managed within the tenant. For more information please see Tenants.

A profile is a specific view on the flow data. The profile is defined by its **name**, **parent profile**, **type** and one or more **profile filters**. You can switch between the available profiles using the profiles menu on the left side of the page.



Profiles page

Profile Types

A profile can be either of type **History** or **Continuous**. A history profile starts and ends back in the past and remains static. It neither grows nor expires. A continuous profile may start in the past and is continually updated while new flow data becomes available. It grows dynamically and may have its own expire values set. Old data expires after a given amount of time or when a certain profile size is reached. Additionally a profile can be created as a **Shadow** profile, which means no flow data is collected, and therefore saves disk space. A shadow profile accesses the data of its parent profile when data processing is done with the proper profile filters applied first. A special type of profile is profile **All Sources**. This profile is on the top of the profiles hierarchy. It contains all flow data collected and cannot be deleted. All profiles in FMC are generated from data collected to profile All Sources - i.e. they are subprofiles of All Sources. For this reason, every profile but All Sources has its parent profile defined. It means it is built from data of its parent profile.

ⓘ **Note**

Parent profile of root profiles is profile All Sources.

Summary

1. Continuous
   - Contains flow data
   - Has dedicated expire values
2. History
   - Contains flow data
   - Starts and ends at defined time
3. Continuous / Shadow
   - Contains no flow data
   - Inherits expire values from parent profile
4. History / Shadow
   - Contains no flow data
   - Starts and ends at defined time

Profile Types by Granularity

A profile can be of one the following types, which might differ with granularity, graph data collection, graph data history length etc.

5-minute profiles

- 5-minute granularity of flow data and graph - 6-month history
- 1-day granularity of flow data and graph - 5-year history
- graph data are available for All, TCP, UDP, ICMP and other traffic
- graph data are available for flows, packets and traffic
- can be built from history data
- its subprofile can be of any type

1-minute profiles

- 1-minute granularity of flow data and graph - 1-month history
- 1-day granularity of flow data and graph - 1-year history
- graph data are available for All traffic
- graph data are available for flows, packets and traffic
- can not be built from history data
- its subprofile can be 1-min and 30-sec profile

30-second profiles

- 1-minute granularity of flow data and graph - 1-month history
- 1-day granularity of flow data and graph - 1-year history
- graph data history length is one year
- graph data are available for All traffic
- graph data are available for flows, packets and traffic
- can not be built from history data
- its subprofile can be 1-min and 30-sec profile

Profile Channels

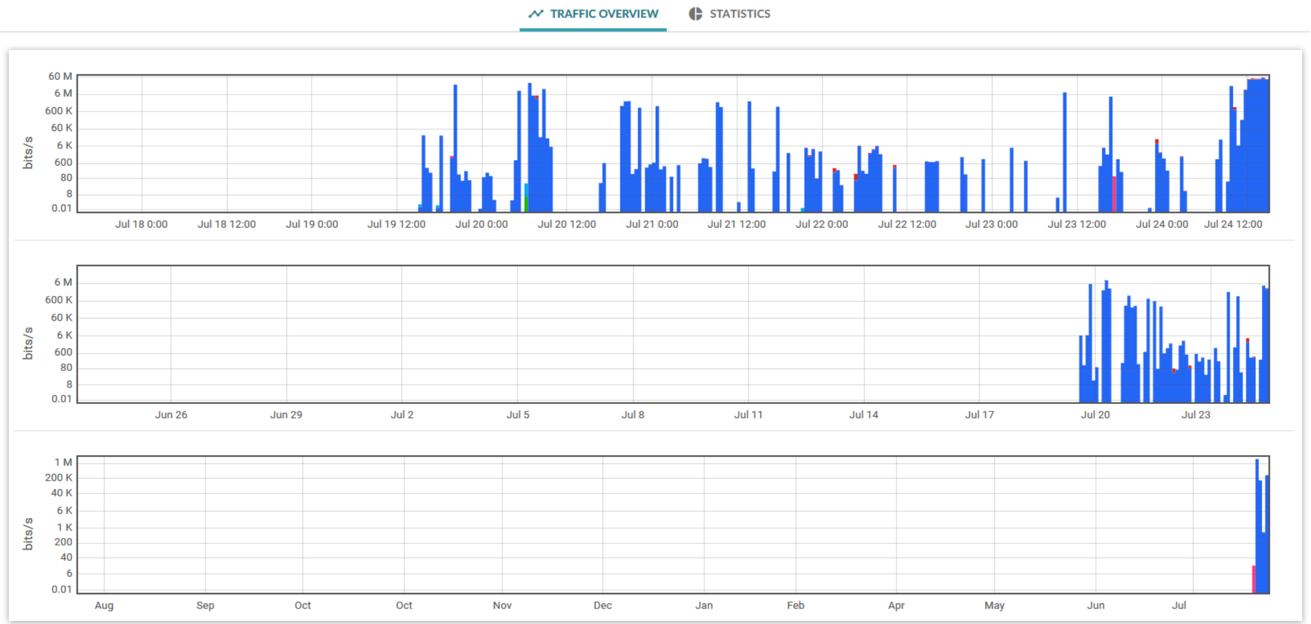
A profile contains one or more profile channels. A profile channel is defined by its channel filter, color, sign and order in which the channel is displayed in the graph. A channel is based on one or more parent channels. Each channel can contain following data entities: captured flows, charts of bytes, packets and flows (**Traffic charts**) and graphs of NPM metrics (**NPM charts**). In default, all entities are enabled for new channel and can be disabled in channel options to save CPU performance or storage.

Profile examples: user or service protocols (http, ftp, smtp, dns etc.), web server communication, upload/download on the company backbone etc.

Overview

The **Overview** page provides a basic view of the recorded data in the selected profile. There is an interactive legend under the chart which makes you able to switch the particular channels or NPM metrics on and off (by clicking the channel icon). The upper pane allows to switch among the **Traffic**, **Packets** and **Flows** views which show measured number of transferred bits, packets and flows. If a continuous profile is selected, the page is automatically refreshed every 5 minutes. This makes you able to have always fresh data in your web browser. By clicking a chart, you can switch to the **Analysis** section where you do further work with data.

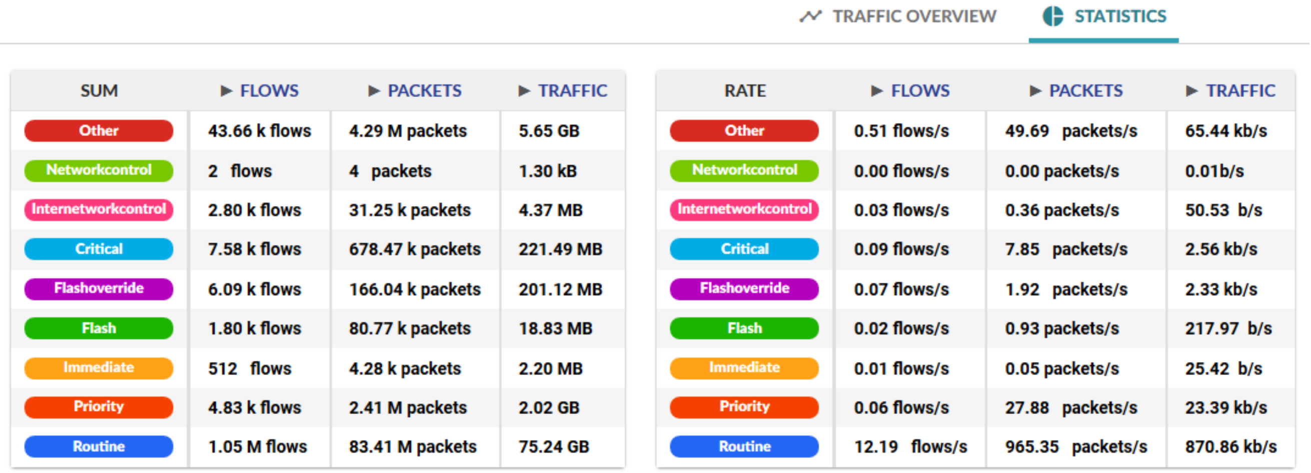
There is a chart displaying a day overview at the top of the page. Below you can switch between **Traffic overview** and **Statistic** tabs. The first tab displays three charts with the week, month and year overview, the second one displays tables with last 24 hours statistics.



Profiles - View

The statistic tables display summary and rate of flows, packets, transferred bits and NPM statistics. Each row corresponds to one channel in the profile. Each row starts with a box and its color matches the chart data color of this channel.

The first table displays totals while the second one displays average transfer rate per second. These values are automatically scaled to best suiting units k, M and G (multiples of 1000). The columns **Flows**, **Packets** and **Traffic** can be displayed in simple or extended mode by clicking the column's header. The extended mode shows concern of particular network protocols in the total. The last table displays average values of **NPM statistics**. The NPM statistics are recorded for every 30 seconds or 5 minutes regarding the profile type as an average of all related flows. The value in table is taken as an average of all recorded values in the displayed interval. The extended mode shows maximal values of NPM statistics. The maximal value is computed as a maximum of all recorded values in the displayed interval.



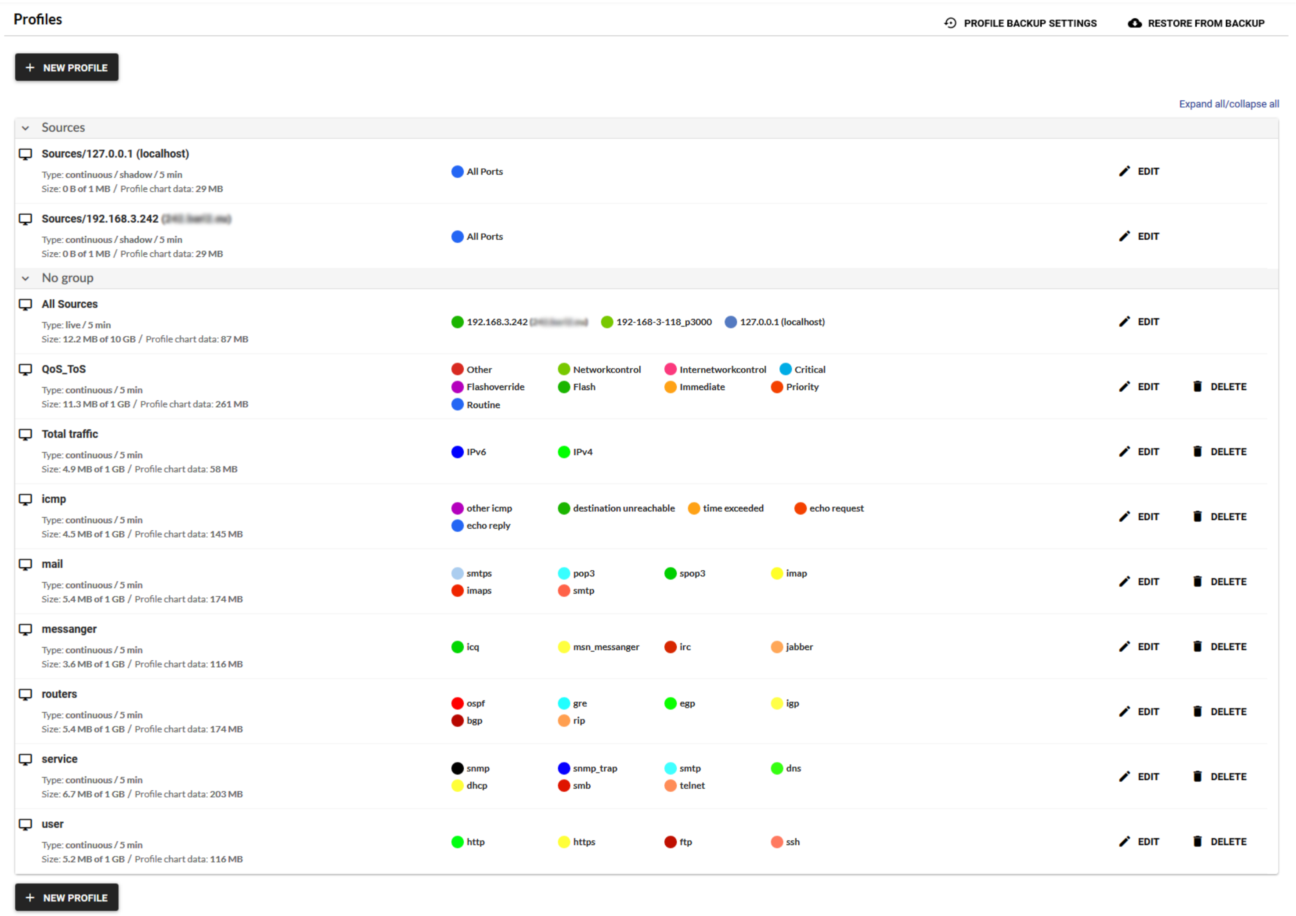
SUM	▶ FLOWS	▶ PACKETS	▶ TRAFFIC
Other	43.66 k flows	4.29 M packets	5.65 GB
Networkcontrol	2 flows	4 packets	1.30 kB
Internetworkcontrol	2.80 k flows	31.25 k packets	4.37 MB
Critical	7.58 k flows	678.47 k packets	221.49 MB
Flashoverride	6.09 k flows	166.04 k packets	201.12 MB
Flash	1.80 k flows	80.77 k packets	18.83 MB
Immediate	512 flows	4.28 k packets	2.20 MB
Priority	4.83 k flows	2.41 M packets	2.02 GB
Routine	1.05 M flows	83.41 M packets	75.24 GB

RATE	▶ FLOWS	▶ PACKETS	▶ TRAFFIC
Other	0.51 flows/s	49.69 packets/s	65.44 kb/s
Networkcontrol	0.00 flows/s	0.00 packets/s	0.01b/s
Internetworkcontrol	0.03 flows/s	0.36 packets/s	50.53 b/s
Critical	0.09 flows/s	7.85 packets/s	2.56 kb/s
Flashoverride	0.07 flows/s	1.92 packets/s	2.33 kb/s
Flash	0.02 flows/s	0.93 packets/s	217.97 b/s
Immediate	0.01 flows/s	0.05 packets/s	25.42 b/s
Priority	0.06 flows/s	27.88 packets/s	23.39 kb/s
Routine	12.19 flows/s	965.35 packets/s	870.86 kb/s

Profiles - Statistic

Profile Modification

Individual profiles can be created, updated and deleted on the **Edit Profiles** page. There is overview table which lists all the profiles and their channels. New profile can be added using **New profile** button. This button opens a dialog box where you can enter new profile preferences. Fill the form and press the **Save** button.



Profiles

PROFILE BACKUP SETTINGS   RESTORE FROM BACKUP

+ NEW PROFILE

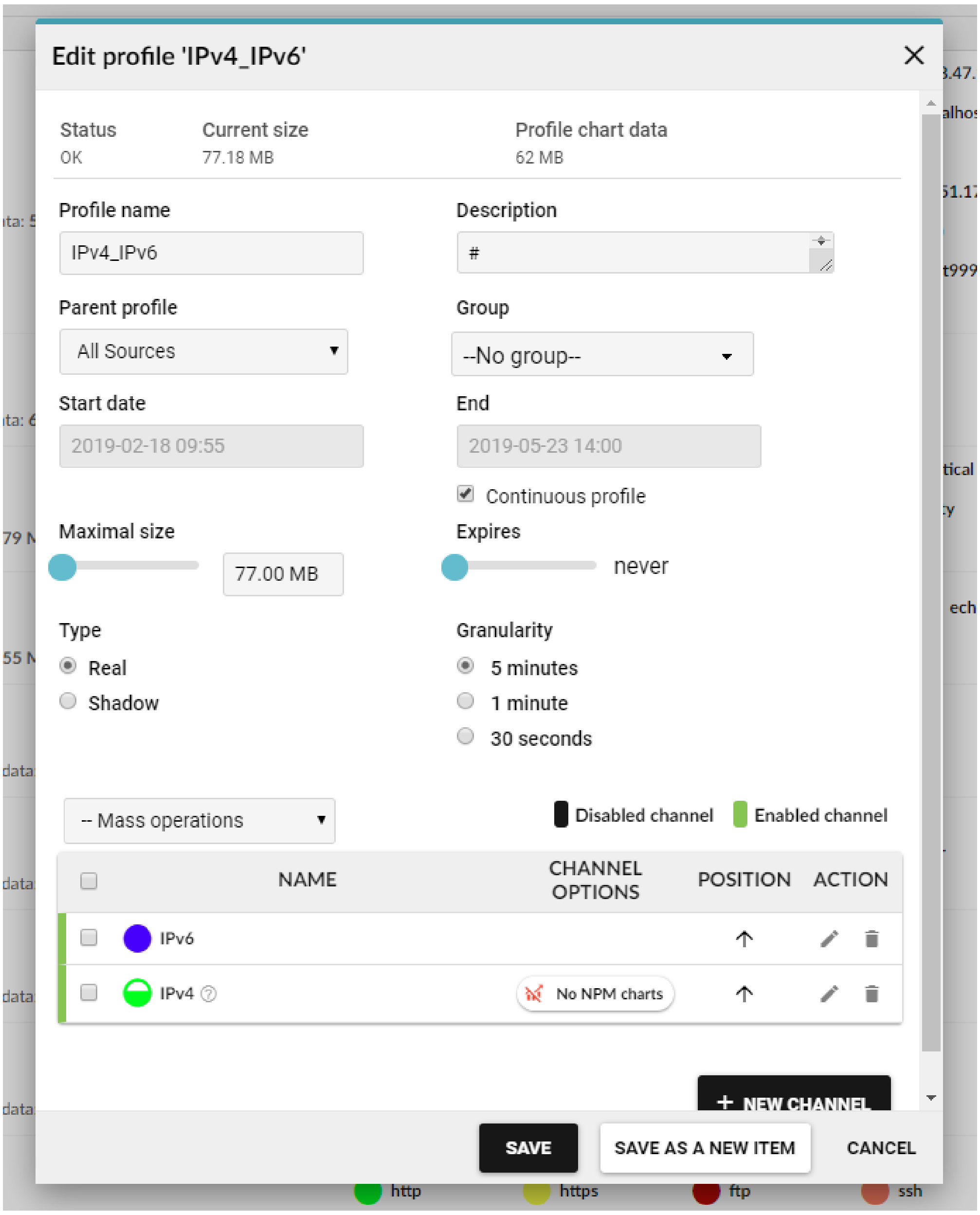
Expand all/collapse all

Sources		
Sources/127.0.0.1 (localhost) Type: continuous / shadow / 5 min Size: 0 B of 1 MB / Profile chart data: 29 MB	● All Ports	EDIT
Sources/192.168.3.242 [redacted] Type: continuous / shadow / 5 min Size: 0 B of 1 MB / Profile chart data: 29 MB	● All Ports	EDIT
No group		
All Sources Type: live / 5 min Size: 12.2 MB of 10 GB / Profile chart data: 87 MB	● 192.168.3.242 [redacted] ● 192-168-3-118_p3000 ● 127.0.0.1 (localhost)	EDIT
QoS_ToS Type: continuous / 5 min Size: 11.3 MB of 1 GB / Profile chart data: 261 MB	● Other ● Networkcontrol ● Internetworkcontrol ● Critical ● Flashoverride ● Flash ● Immediate ● Priority ● Routine	EDIT DELETE
Total traffic Type: continuous / 5 min Size: 4.9 MB of 1 GB / Profile chart data: 58 MB	● IPv6 ● IPv4	EDIT DELETE
icmp Type: continuous / 5 min Size: 4.5 MB of 1 GB / Profile chart data: 145 MB	● other icmp ● destination unreachable ● time exceeded ● echo request ● echo reply	EDIT DELETE
mail Type: continuous / 5 min Size: 5.4 MB of 1 GB / Profile chart data: 174 MB	● smtps ● pop3 ● spop3 ● imap ● imaps ● smtp	EDIT DELETE
messanger Type: continuous / 5 min Size: 3.6 MB of 1 GB / Profile chart data: 116 MB	● icq ● msn_messanger ● irc ● jabber	EDIT DELETE
routers Type: continuous / 5 min Size: 5.4 MB of 1 GB / Profile chart data: 174 MB	● ospf ● gre ● egp ● igp ● bgp ● rip	EDIT DELETE
service Type: continuous / 5 min Size: 6.7 MB of 1 GB / Profile chart data: 203 MB	● snmp ● snmp_trap ● smtp ● dns ● dhcp ● smb ● telnet	EDIT DELETE
user Type: continuous / 5 min Size: 5.2 MB of 1 GB / Profile chart data: 116 MB	● http ● https ● ftp ● ssh	EDIT DELETE

+ NEW PROFILE

Profiles

Profiles can be modified by clicking on the **Edit** button. Parent profile can be changed only for new profile. In continuous profile you can add and delete particular channels. If you add a new channel to an existing profile, the data from the past is not processed for this channel. All the performed changes become evident immediately after clicking the **Save** button. A profile can be deleted by clicking the **Delete** button in the overview table.



Edit profile 'IPv4_IPv6'

Status: OK
Current size: 77.18 MB
Profile chart data: 62 MB

Profile name: IPv4_IPv6
Description: #
Parent profile: All Sources
Group: --No group--
Start date: 2019-02-18 09:55
End: 2019-05-23 14:00
☑ Continuous profile
Maximal size: 77.00 MB
Expires: never

Type
● Real
○ Shadow

Granularity
● 5 minutes
○ 1 minute
○ 30 seconds

-- Mass operations

Disabled channel · Enabled channel

□	NAME	CHANNEL OPTIONS	POSITION	ACTION
□	IPv6		↑	✎ 🗑
□	IPv4	No NPM charts	↑	✎ 🗑

Profile configuration

Creating Profiles

For a new profile, click the **New profile** button.

You can join particular profiles to groups and thereby you can reach better arrangement in the profiles menu. Choose either an existing group or create a new one. Insertion of profile to a group affect only its position in the table, nothing else (the rest of its features remain untouched).

Fields **Start date** and **End** determine range of data in the profile. Each profile is derived from its parent profile, and therefore the start and end dates must fit the range of parent profile.

- If you fill the **Start date** field and check the **Continuous profile** checkbox, continuous profile is created. Data from the past is automatically processed from the Start date to the present according to the profile rules. Then data is stored in the profile's database providing it is not a shadow profile.
- If you fill both **Start date** and **End** a history profile is created automatically.
- Field parent profile can be set only during creation of new profile. Its value determines a set of parent channels in channel definition form.

Maximal size defines the maximal size of profile data. If the profile data reach this limit, the oldest data are overwritten by the new data. The same applies for **Expires** limit defining the maximum data age.

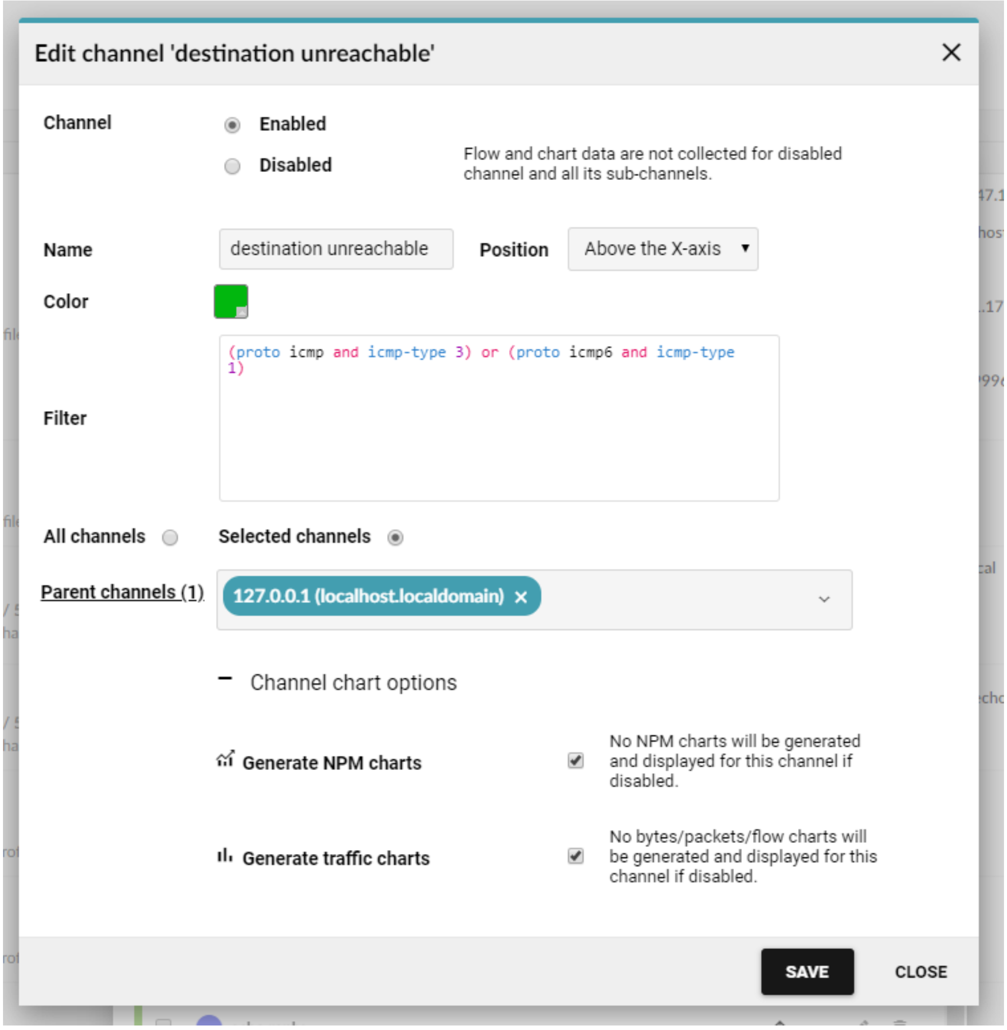
The **Granularity** option is used for selecting the Profile granularity.

The channel table follows below. It contains list of all profile channels and their state. In the **Name** column, there is a name of the channel together with its color. The color circle can be full (all data entities are enabled), half-full (some data entities are disabled) or empty (the channel is disabled). The **Channel Options** column shows which data entities are disabled. Column **Position** shows whether the channel chart will be drawn above or below the x-axis. In the **Action** column, there are icons for channel edit and delete operation.

Creating Channels

You can add arbitrary number of channels to a profile. Each channel corresponds to one color in the chart. New channel can be added by clicking the **New channel** button.

Parameters **Color** and **Position** set up data appearance in the chart. Processed data is defined using **Filter** and **Parent channels** fields. The Filter field uses the same syntax and rules as the filter form on the page Analysis (it will be discussed later). In the field Parent channels there are source data for channel configured. Either **All channels** or **Selected channels** option can be selected. Option All channels will always assign all parent channels, even those created later. Option Selected channels allows to define the exact set of parent channels. **Channel charts options** section can be expanded for control which data entities will be processed in the channel. The channel can be **Disabled** completely by the select box at the top of the form. The disabled channel is not processed at all - no data are captured and no charts are drawn. **IMPORTANT:** if the channel is disabled, than also all its subchannels are disabled!



Edit channel 'destination unreachable' ✕

Channel ● Enabled ○ Disabled

Flow and chart data are not collected for disabled channel and all its sub-channels.

Name: destination unreachable

Position: Above the X-axis ▾

Color: 🟩

Filter:

```
(proto icmp and icmp-type 3) or (proto icmp6 and icmp-type
1)
```

All channels ○ Selected channels ●

Parent channels (1): 127.0.0.1 (localhost.localdomain) ✕

− Channel chart options

Generate NPM charts ☑ No NPM charts will be generated and displayed for this channel if disabled.

Generate traffic charts ☑ No bytes/packets/flow charts will be generated and displayed for this channel if disabled.

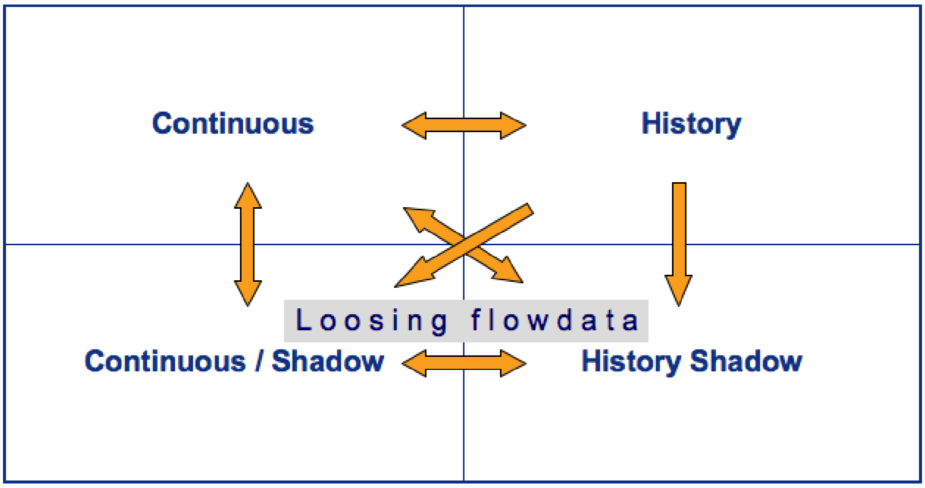
SAVE CLOSE

Channels configuration

Order of channels in the list can be changed by drag and drop. Creation of a new profile is finished by clicking the **Save** button. Then calculation of profile data starts. Length of calculation process depends on the selected time range. Until the generation is not complete, charts do not display any data for this profile.

Converting Profiles

Profile may be converted into another type as desired. However, not all conversions are possible. The picture below shows and explains the possible conversions.



Profile conversion scheme

By switching profile type between continuous and history you may temporary stop collecting data for a profile or continuing to collect data from a stopped profile. Note, that you will loose all flow data, when a profile is converted to a shadow profile. When switching back, the data recording resumes at the time of switching.

Predefined Profiles

In the Flowmon Monitoring Center there are several predefined profiles, that provide information about history of common protocols and services detected on the monitored link. For example, there are user protocols (HTTP, HTTPS, FTP, SSH), service protocols (SNMP, DNS, DHCP, SAMBA) and many others. The protocols detection is based on port numbers of captured flows, defined by IANA organization (http://www.iana.org/assignments/port-numbers). The most of predefined services are defined over both, TCP and UDP protocols. However, some protocols typically use only one of them (e.g. HTTP / TCP port 80). This is frequently exploited by the more experienced users, who can use the port 80/UDP to illegally tunnel their traffic (incorrectly configured firewall might accept the traffic on the port 80/UDP). For this reason, it is very useful for each administrator to see such traffic and that's why all predefined protocols are defined for both, TCP and UDP protocols.

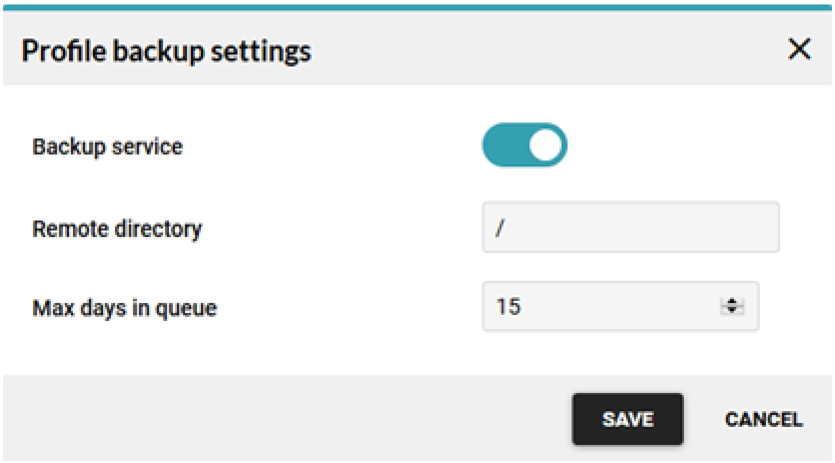
Profiles Backup

Profiles in Flowmon Monitoring Center can be backed up to an external storage (configured in Configuration center, see chapter External Data Storage). The backup is performed every day few minutes after midnight when all data from previous day are copied to external storage. Multiple Flowmon devices can backup data to the same external storage. Backed up data are marked with HW ID of the source Flowmon device. If backup fails, data remains in queue and Flowmon tries to copy them again next day together with next-day data. The maximum length of the queue in days might be configured.

Backed up data may be restored for selected profile, source Flowmon device and time interval.

Data are restored in the form of history profile with user-defined name and group.

To enable this functionality, the External storage must be configured in Configuration center. Then it can be enabled in dialog box **Profile backup settings** which can be shown by clicking on button with the same name. Here, **Remote directory** on external storage can configured. This directory will be used for storing backup. Option **Max days in queue** defines for how long will system keep unsuccessfully copied data in queue. If the data are older, they are removed and system will not try to backup them again.



Profile backup settings

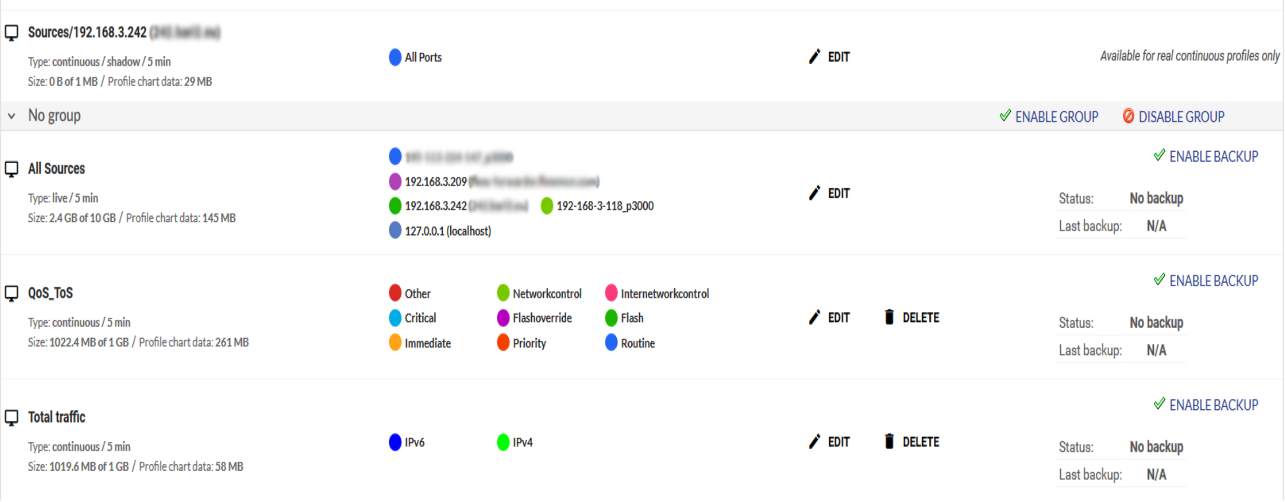
Backup service

Remote directory: /

Max days in queue: 15

Profile backup settings

Each profile can be enabled or disabled for backup - buttons **Enable backup** and **Disable backup**. These buttons are available for group as well. They just enable or disable backup for all profiles in this group. When backup for profile is enable, current backup status will be shown including last backup time.



Sources/192.168.3.242 [redacted]
Type: continuous / shadow / 5 min
Size: 0 B of 1 MB / Profile chart data: 29 MB
● All Ports
EDIT
Available for real continuous profiles only

No group — ✓ ENABLE GROUP — DISABLE GROUP

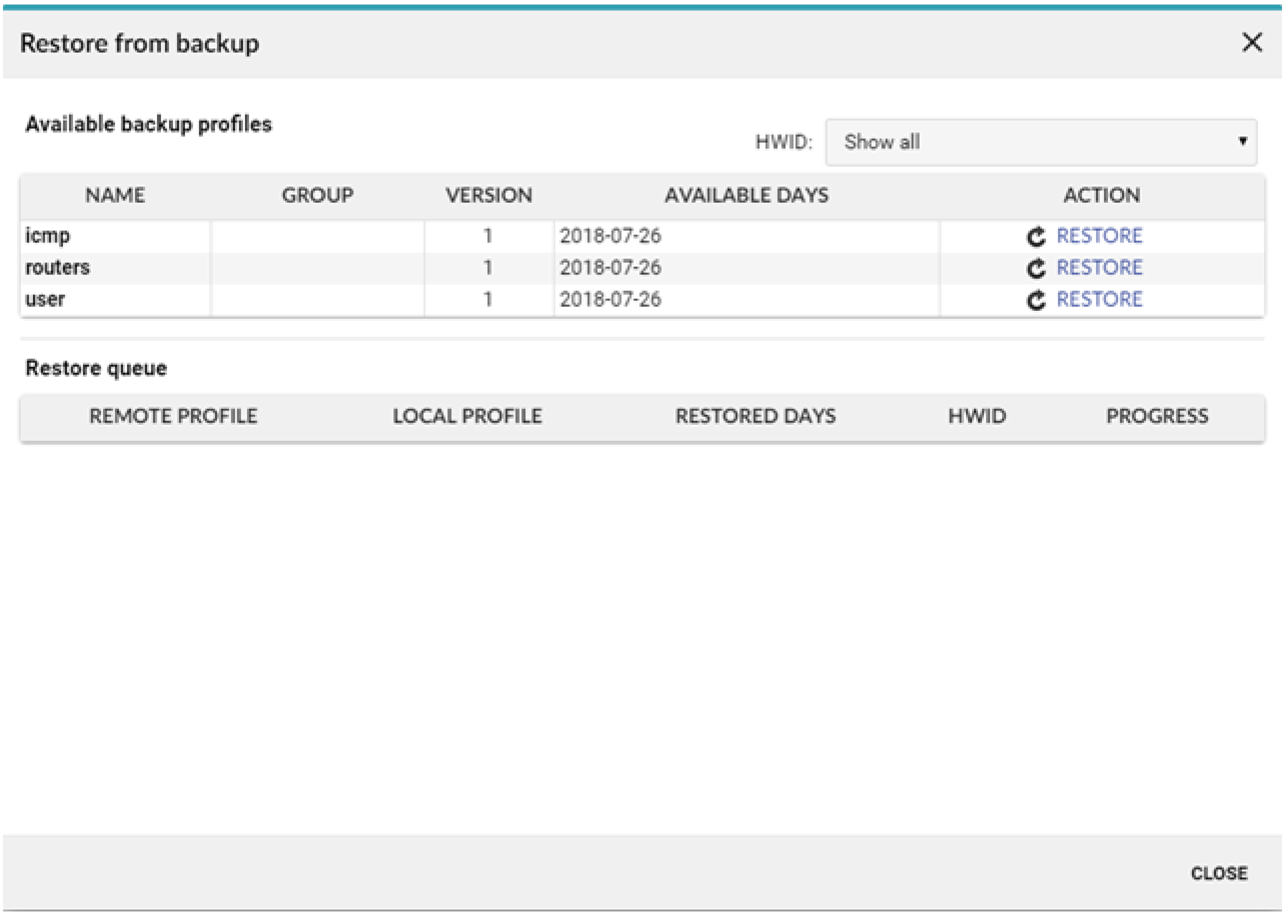
All Sources
Type: live / 5 min
Size: 2.4 GB of 10 GB / Profile chart data: 145 MB
● [redacted]
● 192.168.3.209 [redacted]
● 192.168.3.242 [redacted] ● 192-168-3-118_p3000
● 127.0.0.1 (localhost)
EDIT
✓ ENABLE BACKUP
Status: No backup
Last backup: N/A

QoS_ToS
Type: continuous / 5 min
Size: 1022.4 MB of 1 GB / Profile chart data: 261 MB
● Other ● Networkcontrol ● Internetworkcontrol
● Critical ● Flashoverride ● Flash
● Immediate ● Priority ● Routine
EDIT DELETE
✓ ENABLE BACKUP
Status: No backup
Last backup: N/A

Total traffic
Type: continuous / 5 min
Size: 1019.6 MB of 1 GB / Profile chart data: 58 MB
● IPv6 ● IPv4
EDIT DELETE
✓ ENABLE BACKUP
Status: No backup
Last backup: N/A

Profiles - backup column

Profiles can be restored in dialog box opened by button **Restore from backup**. In section **Available backup profiles**, profiles available for restore are shown. When first opened, loading of list of profiles for restore might take a few minutes. Next time, it should be much faster as it is already cached. In **HWID** drop down menu, the particular backed up Flowmon device can be selected. Then only profiles backed up from this device will be shown. Below the Restore queue is displayed including current restore status. Profile restore can be done by clicking on **Restore** button. Dialog box Restore settings will be displayed.



Restore from backup ✕

Available backup profiles

HWID: Show all ▾

NAME	GROUP	VERSION	AVAILABLE DAYS	ACTION
icmp		1	2018-07-26	RESTORE
routers		1	2018-07-26	RESTORE
user		1	2018-07-26	RESTORE

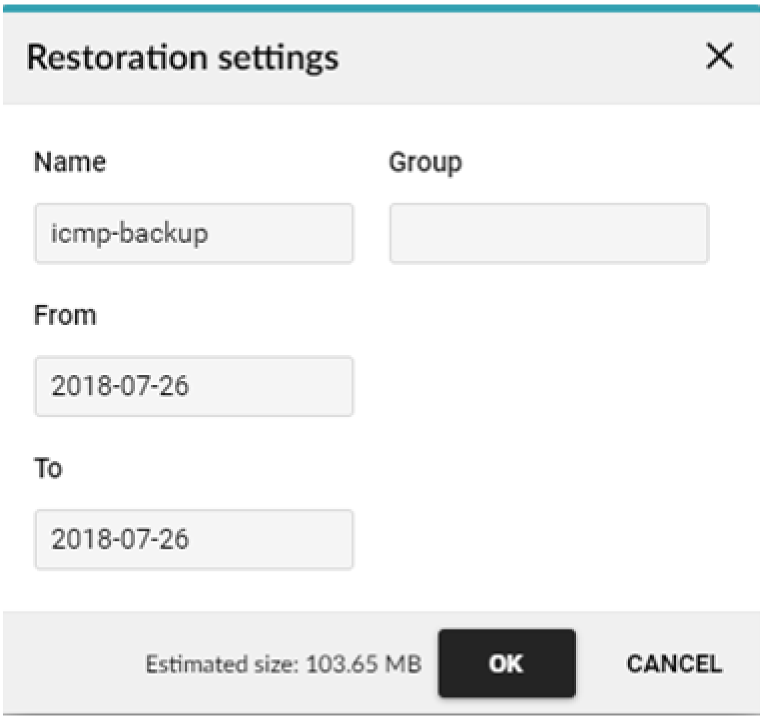
Restore queue

REMOTE PROFILE	LOCAL PROFILE	RESTORED DAYS	HWID	PROGRESS

CLOSE

Restore from backup

Here, new name of profile can be defined including its group (i.e. the restored profile will be named by new name and will be located in provided group). Next, time interval for restored data must be specified.



Restoration settings

Name: icmp-backup

Group:

From: 2018-07-26

To: 2018-07-26

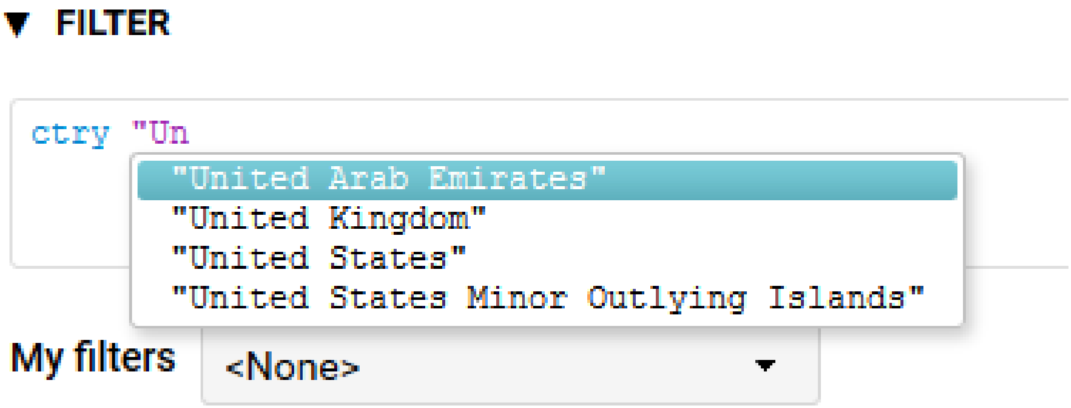
Estimated size: 103.65 MB

Restore settings

Filter Syntax

The filter syntax is similar to the well known pcap library used by tcpdump. The filter can span several lines. Anything after a '#' is treated as a comment and ignored to the end of the line. There is virtually no limit in length of the filter expression. All keywords are case independent (e.g. IP is the same as ip), unless noted otherwise. The strings are enclosed in double quotes. String values are case sensitive (e.g. "windowsupdate.COM" is not the same as "windowsupdate.com").

For several keywords you can use autocomplete function for entering the desired value - see the picture below.



```
ctry "Un
"United Arab Emirates"
"United Kingdom"
"United States"
"United States Minor Outlying Islands"
```

My filters <None>

Autocomplete function

Filter consists of individual expressions. Expressions can be connected with logical operators “and” or “or”. When two expressions are connected with logical operator “and”, the filtered data must satisfy conditions in both expressions in order to be included in results. Logical operator “or” means that the data must match at least one of the expressions. All data matching the expression can be excluded by applying operator “not”. Brackets can be used to create more complex filters:

```
<expression>
<expression> and <expression>
<expression> or
<expression> not
<expression>
( <expression> )
```

See the following subchapters with possible content of the <expression> element, i. e. primitives.

Any

Use **any** as a dummy filter. Use **not any** to block all flows.

Protocol Primitives

Protocol version

- **inet** or **ipv4** for IPv4
- **inet6** or **ipv6** for IPv6

Protocol

- **proto <protocol>** where <protocol> can be any known protocol such as **TCP**, **UDP**, **ICMP**, **ICMP6**, **ARP**, **GRE**, **ESP**, **AH** etc.
- **proto <num>** where <num> is the protocol number (e.g. 1 for ICMP).

Protocol and protocol version examples

- **inet6** - matches only IPv6 communication.

The following four filters have all the same meaning.

- **inet6 and proto udp** - matches only UDP communication over IPv6.
- **inet6 and proto 17** - because UDP = 17.
- **ipv6 and proto 17** - because inet6 and ipv6 are interchangeable.
- **IPV6 AND PROTO 17** - because the expressions are **not** case sensitive.

- **proto icmp or proto udp** - matches both ICMP and UDP.
- **(proto icmp or proto udp) and ipv4** - matches both ICMP and UDP communication only over IPv4.
- **ipv4 and (proto icmp or proto udp)** - is identical with the previous (the order does not matter in this case).
- **ipv4 and proto icmp or proto udp** - ambiguous, brackets are missing (UDP would be using both IPv4 and IPv6).
- **not (proto tcp or proto udp or proto icmp)** - excludes TCP, UDP and ICMP communication (ARP, ICMP6, IGMP and other protocols can be explored).

IP Address Primitives

IP address

- **[src|dst] IP <ipaddr>** or **[src|dst] HOST <ipaddr>** with <ipaddr> as any valid IPv4 or IPv6 address. [**src**|**dst**] defines the IP address to be selected - SRC for source, DST for destination. Omitting [**src**|**dst**] means any direction (it is equivalent to “SRC or DST”).
- **[src|dst]** IP addresses, networks, ports, AS numbers etc. can be specifically selected using a direction qualifier, such as src or dst. These can also be used in combination with “and” and “or” (e.g. “as src and dst ip”).

IP address - examples

- **ip 192.168.2.4** - matches specific IP address (both source and destination).
- **src or dst ip 192.168.2.4** - is identical to the previous.
- **src ip 192.168.2.4** - matches specific source IP address.
- **src host 192.168.2.4** - is identical to the previous (IP and host are interchangeable).
- **proto tcp and (src ip 192.168.2.3 or dst ip 192.168.0.1)** - matches TCP communication with either first source address or second destination address.

List of IP addresses

- **[src|dst] IP IN [<iplist>]** or **[src|dst] HOST IN [<iplist>]** where iplist is a space-separated list of individual <ipaddr>.

List of IP addresses - examples

- **src ip in [192.168.2.3 192.168.2.4]** - matches records with these two addresses as sources.
- **ip in [192.168.2.3 192.168.2.4] and proto tcp** - matches only TCP communication of these addresses.

Network Primitives

Network

- **[src|dst] net a.b.c.d m.n.r.s** - selects the IPv4 network a.b.c.d with netmask m.n.r.s.
- **[src|dst] net <net>/<num>** with <net> as a valid IPv4 or IPv6 network and <num> as maskbits. The number of mask bits must match the appropriate address family in IPv4 or IPv6. Networks may be abbreviated such as 172.16/16 if they are unambiguous.
- **[src|dst] net in [<ip/masklist>] -** where **<**ip/masklist> is list of subnet addresses (see examples)

Network - examples

- **src net 192.168.0.0/16** - matches IPs starting with 192.168 (first 16 bits of the IP address are masked).
- **src net 192.168.0.0 255.255.0.0** - is identical to the previous (first 16 bits are 1s).
- **src net 192.168.0.0 255.255.255.240** - matches IPs in a range from 192.168.0.0 to 192.168.0.15 (last number of mask 240 is 1111 0000 in binary).
- **src net 192.168.0.0 255.255.255.240 and not ip [192.168.0.14 192.168.0.15]** - matches IPs in a range from 192.168.0.0 to 192.168.0.13.
- **src net in [192.168.10.0/24, 192.168.20.0/24] and dst net in [192.168.50.0/24, 192.168.60.0/24]** - matches IPs with source of subnet **192.168.10.0/24** or **192.168.20.0/24** and destination subnet **192.168.50.0/24** or **192.168.60.0/24**

Port Primitives

Port

- **[src|dst] PORT [<comp>] <num>**
- **[src|dst] PORT IN [<portlist>]**
- **[src|dst] PORT "<portname>"**

The <portlist> is a space-separated list of individual port numbers. The <num> is a valid port number. The <portname> is a name of a service assigned to a specific port number by IANA. Use autocomplete function to enter the service name.

The <comp> is a comparator. The following comparators are supported:

=, **==**, **>**, **<**, **EQ**, **LT**, **GT**. If <comp> is omitted, '=' is assumed.

Port - examples

- **dst port 110** - matches destination port 110 (pop3).
- **dst port "pop3"** - is identical to the previous (“pop3” is a text name for this port).
- **port in [20, 21]** - matches FTP communication.
- **src port < 1024 and not port in [80,443]** - matches well-known source ports (0-1023) in use, but ignores HTTP(S).
- **dst port > 1023 and dst port < 49152 and proto udp** - matches registered destination ports (1024-49151) in use over UDP.

ICMP

- **icmp-type <num>**
- **icmp-code <num>**

with <num> as a valid icmp type/code. This automatically implies **proto icmp**.

Router ID

- **engine-type <num>**
- **engine-id <num>**

with <num> as a valid router engine type/id (0..255).

HTTP Primitives

HTTP hostname

- **hhost [<strcomp>] "<string> with <string> as a part or complete HTTP hostname."**

The <strcomp> is a comparator. The following comparators are supported:

= - compared strings are identical.

> - <string> begins with a compared string.

< - <string> ends with a compared string.

If <comp> is omitted, compared string is a substring of <string>.

HTTP URL

- **hurl [<strcomp>] "<string>"** with <string> as a part or complete URL.

HTTP - Operating System in User Agent

- **hos "<string>"** with <string> as a name of operating system (use the autocomplete function).

HTTP - Operating System Major Version

- **hosmaj [<comp>] <num>** with <num> as a major version number.

HTTP - Operating System Minor Version

- **hosmin [<comp>] <num>** with <num> as a minor version number.

HTTP - Operating System Build Number

- **hosbld [<comp>] <num>** with <num> as a build number.

HTTP - Client Application in User Agent

- **happ "<string>"** with <string> as a name of client application (use the autocomplete function).

HTTP - Client Application Major Version

- **happmaj [<comp>] <num>** with <num> as a major version number.

HTTP - Client Application Minor Version

- **happmin [<comp>] <num>** with <num> as a minor version number.

HTTP - Client Application Build Number

- **happbld [<comp>] <num>** with <num> as a build number.

HTTP - HTTP Method

- **hmethod "<string>"** with <string> as a name of HTTP method (use the autocomplete function).

HTTP - HTTP Return Code

- **hrcode [<comp>] <num>** with <num> as a return code.

Autonomous System Numbers Primitives

Autonomous system numbers

- [**src**|**dst**|**prev**|**next**] **as [<comp>] <num>** - selects source, destination, previous, next or any AS number with <num> as any valid as number. 32bit AS numbers are supported. If **<comp>** is omitted, '=' is assumed.
- [**src**|**dst**|**prev**|**next**] **as in [<ASlist>]** - an AS number can be compared against a known list, where <ASlist> is a space or comma separated list of individual AS numbers.

Autonomous system number - examples

- **as 15169** - includes whole communication involving Google LLC AS (15169).
- **not src as 8068** - excludes communication from Microsoft Corporation AS (8068).

VLAN labels

- [**src**|**dst**] **vlan <num>** with <num> as any valid VLAN label.

User identity of IP

- [**src**|**dst**] **uid <user ID>** with <user ID> as a user identifier provided by DHCP, VPN, directory service etc. via syslog.

Country of origin of IP

- **[src|dst] ctry "<country name>"**
- [**src**|**dst**] **ctry <num>**

with <country name> as a name of country. Use autocomplete function to enter the name of a country. The <num> is number of country according to ISO 3166-2.

Flow Source Identification

- **flowident "<string>"** with <string> as a flow source identification (use the autocomplete function).

TCP Flags Primitives

TCP flags

tcpflags [=] "<flagstring>" with flagstring in the following format:

- flagstring ::= <flagstringexp>
- <flagstringexp> ::= <exp>
- <flagstringexp> ::= <exp-and>
- <flagstringexp> ::= <exp-or>
- <exp> ::= <flag> | <exp><flag>
- <exp-and> ::= <flag> | <exp-and> "&" <flag>
- <exp-or> ::= <flag> | <exp-or> "|" <flag>

<flag> - "A" | "S" | "F" | "R" | "P" | "U" | "C" | "E" | "X"

<flag> has the following meaning:

- **A** - ACK **S** - SYN **F** - FIN
- **R** - Reset
- **P** - Push
- **U** - Urgent
- **C** - Congestion Window Reduced
- **E** - ECN-Echo
- **X** - All flags on

<exp>, <exp-and> and <exp-or> have the following meaning:

- The **<exp>** filter selects flows containing all flags listed in <exp>. To include these flags only, use operator "=".
- The **<exp-and>** is equivalent to <exp>.
- The **<exp-or>** filter selects flows containing at least one of the flags listed in <exp-or>. To include these flags only, use operator "=".

TCP Flags - examples

- **tcpflags S** - matches any flow which includes S flag in TCP flags (e.g. ...AP.S. or ...A..SF).
- **tcpflags = S** - matches records with only the SYN flag set (i.e...... S.).
- **tcpflags** "**S|F**" - either S or F flag must be present.
- **tcpflags = "A&P&F"** - only specified flags (...AP..F) are allowed.

Extended TCP

- **tcpttl [=|==|<|>|eq|lt|gt] <number>** - filters by TCP TTL (Time to live).
- **tcpwinsize [=|==|<|>|eq|lt|gt] <number>** - filters by TCP window size.
- **tcpsynsize [=|==|<|>|eq|lt|gt] <number>** - filters by TCP syn packet size.

Next Hop IP Primitive

- **next ip <ipaddr>** with <ipaddr> as IPv4/IPv6 IP address of next hop router.

Next-hop router's IP in the BGP domain

- **bgpnext ip <ipaddr>** with <ipaddr> as IPv4/IPv6 next-hop router's IP in the BGP domain.

Router IP Primitive

- **router ip <ipaddr>** - filters the flows according to the IP address of the exporting source (router or probe).

Flow Source Name Primitive

- **source "<sourcename>"** - filters the flows according to the name of exporting source (router or probe). Use autocomplete function to enter the name of source. Only names shown on page "Sources" are supported.

Source ID Primitive

- **sourceid [<comp>] <number>** - filters flows with specific source ID (one exporting device might use multiple source IDs for different exporting engines). Supported for sFlow only.

Interface Primitives

Interface

- **[<inout>] if <num>** - selects input or output interface ID. Omitting [in|out] is equivalent to IN **or** OUT (selects either IN or OUT interfaces). The <num> is SNMP interface number.

Interface - Examples

- **in if 3** - selects input interface #3.

Flow Source Network Interface Name

- **sourceport "<sourcename>":"<interfacename>"** - filters flows exported from network interface <interfacename> on source <sourcename>. Use autocomplete function to enter the name of the source and interface. Only names shown on page "Sources" are supported.

MAC Address Primitive

- **[<in src|in dst|out src|out dst>] mac <addr>** with <addr> any valid MAC. The <mac> can be specified more by using any combinations of a direction specifier as defined by CISCO v9: **in src**, **in dst**, **out src**, **out dst**.

MPLS Labels Primitives

- **mpls label<n> [<comp>] <num>** with <n> as any MPLS label number in range 1..10. It filters exactly specified label<n>.
- **mpls eos [<comp>] <num>** - filters End of Stack label for a given value <num>.
- **mpls exp<n> [<comp>] <bits>** - filters experimental bits of label <n> with <bits> in range 0..7.

TOS Primitives

TOS

- **tos <value>** for the Type of Service. Both ToS numerical values 0..255 and DSCP name strings are supported.

TOS examples

- **not tos "Best Effort & Default"** - excludes the best effort communication.
- **not tos 0** - is identical to the previous (0 stands for the best effort).
- **tos "CS7"** - is the same as **tos 224**

For further information please visit https://en.wikipedia.org/wiki/Type_of_service

NBAR2 Primitives

NBAR2 AppTag

- **apptag "<appname>"**
- **apptag <AppEID>:<AppID>**

with <appname> as a name of application recognized by NBAR2. Use autocomplete function to enter the application name. The <AppEID> is Classification Engine ID and <AppID> is Application ID (defined in RFC 6759 and NBAR2 Protocol Pack).

NBAR2 AppEID

- **appeid <value>** with <value> as a number (0..255).

NBAR2 AppID

- **appid <value>** with <value> as a number (0..16777216).

DNS Primitives

DNS filters

A correct DNS filter should be preceded with keyword "dns" to correctly process only the valid DNS flows (e.g. **dns and dns-qrflag 0**).

DNS ID

- **dns-id [=|==|<|>|eq|lt|gt] <value>** with <value> as a number (0..65535).

DNS question count

- **dns-qcount [=|==|<|>|eq|lt|gt] <value>** with <value> as a number (0..65535).

DNS asnwer count

- **dns-answcount [=|==|<|>|eq|lt|gt] <value>** with <value> as a number (0..65535).

DNS authority count

- **dns-authcount [=|==|<|>|eq|lt|gt] <value>** with <value> as a number (0..65535).

DNS additional count

- **dns-addtcount [=|==|<|>|eq|lt|gt] <value>** with <value> as a number (0..65535).

DNS flags

- **dns-flags [=] "<flagstring>"** with <flagstring> in the following format:
  - flagstring ::= ”"” <flagstringexp> ”"”
  - <flagstringexp> ::= <exp>
  - <flagstringexp> ::= <exp-and>
  - <flagstringexp> ::= <exp-or>
  - <exp> ::= <flag> | <exp><flag>
  - <exp-and> ::= <flag> | <exp-and> "&" <flag>
  - <exp-or> ::= <flag> | <exp-or> "|" <flag>
  - <flag> "AA" | "TC" | "RD" | "RA" | "AD" | "CD"
  - <flag> has the following meaning:

AA - Authoritative Answer Flag

TC - Truncation Flag

RD - Recursion Desired

RA - Recursion Available

AD - Authentic Data

CD - Checking Disabled

<exp>, <exp-and> and <exp-or> have the following meaning:

1. The **<exp>** filter selects flows containing all flags listed in <exp>. To include these flags only, use operator "=".
2. The **<exp-and>** is equivalent to <exp>.
3. The **<exp-or>** filter selects flows containing at least one of the flags listed in <exp-or>. To include these flags only, use operator "=".

- **dns-qrflag [=|==|<|>|eq|lt|gt] <value>**, where value "0" is a DNS Query and "1" is a DNS Response.
- **dns-opcode [=|==|<|>|eq|lt|gt] <value>** with <value> as a DNS operation code.
- **dns-rcode [=|==|<|>|eq|lt|gt] <value>** with <value> as a DNS response code.

DNS question

- **dns-qname [<strcomp>] "<string>"** with <string> as a question name.
- **dns-qtype [=|==|<|>|eq|lt|gt] <value>** with <value> as a question type.
- **dns-qclass [=|==|<|>|eq|lt|gt] <value>** with <value> as a question class.
- **dns-qname1 "<string>"** with <string> as a question name (1st level domain).
- **dns-qname2 "<string>"** with <string> as a question name (1st & 2nd level domain).
- **dns-qname3 "<string>"** with <string> as a question name (1st, 2nd & 3nd level domain).

DNS response

- **dns-rname [<strcomp>] "<string>"** with <string> as a question response name.
- **dns-rtype [=|==|<|>|eq|lt|gt] <value>** with <value> as a response type.
- **dns-rclass [=|==|<|>|eq|lt|gt] <value>** with <value> as a response class.
- **dns-rttl [=|==|<|>|eq|lt|gt] <value>** with <value> as a response TTL.
- **dns-rdata [<strcomp>] "<string>"** with <string> as a response data.
- **dns-rname1 "<string>"** with <string> as a question response name (1st level domain).
- **dns-rname2 "<string>"** with <string> as a question response name (1st & 2nd level domain).
- **dns-rname3 "<string>"** with <string> as a question response name (1st, 2nd & 3nd level domain).
- **dns-rdata1 "<string>"** with <string> as response data (1st level domain). Only for response type CNAME, DNAME, NS, SOA, MX, SRV.
- **dns-rdata2 "<string>"** with <string> as response data (1st & 2nd level domain). Only for response type CNAME, DNAME, NS, SOA, MX, SRV.
- **dns-rdata3 "<string>"** with <string> as response data (1st, 2nd & 3nd level domain). Only for response type CNAME, DNAME, NS, SOA, MX, SRV.

DHCP Primitives

DHCP offered IP address

- **dhcp-offeredip <ip>** with <ip> as the IP address, which DHCP server offered to the host.

DHCP MAC address of host

- **dhcp-hostmac <macaddr>** with <macaddr> as a MAC address of the host.

DHCP message type

- **dhcp-type [=|==|<|>|eq|lt|gt] <value>**, with <value> as a combination of (RFC 2132, RFC 3203, RFC 4388, RFC 6926, draft-ietf-dhc-dhcpv4-active-leasequery-07):

1 - Discover

2 - Offer

3 - Request

4 - Decline

5 - ACK

6 - NAK

7 - Release

8 - Inform

9 - Force Renew

10 - Lease Query

11 - Lease Unassigned

12 - Lease Unknown

13 - Lease Active

14 - Lease Bulk Lease Query

15 - Lease Query Done

DHCP IP address lease time

- **dhcp-leasetime [=|==|<|>|eq|lt|gt] <value>** with <value> as the IP address lease time. Value is specified in seconds.

DHCP server IP address

- **dhcp-servip <ip>** where <ip> is the IP address of the DHCP server.

DHCP server domain name

- **dhcp-domname [<strcomp>] "<string>"** with <string> as the domain name of the DHCP server.

DHCP hostname

- **dhcp-hostname [<strcomp>] "<octalstring>"** with <octalstring> as a combination of:

– **<string>**

– **<octalval>** where <octalval> is a string in the following format \&nnn, where *nnn* is the octal number in range 0..255.

DHCP requested IP address

- **dhcp-ipreq <ip>** with <ip> as the requested IP address.

Samba Primitives

Samba operation code version 1

- **smb1-cmd [=|==|<|>|eq|lt|gt] <smbopcode1>** with <smbopcode1> as a samba operation code version 1.

Samba operation code version 2

- **smb2-cmd "<flagstring>"** with <flagstring> in following format:

– flagstring ::= "" <flagstringexp> ""

– <flagstringexp> ::= <exp>

– <flagstringexp> ::= <exp-and>

– <flagstringexp> ::= <exp-or>

– <exp> ::= <flag> | <exp><flag>

– <exp-and> ::= <flag> | <exp-and> "&" <flag>

– <exp-or> ::= <flag> | <exp-or> "|" <flag>

– <flag> - "NE" | "SS" | "LO" | "TC" | "TD" | "CR" | "CL" | "FL" | "RE" | "WR" | "LC" | "IO" | "CA" | "EC" | "QD" | "CN" | "QI" | "SI" | OB" | "EN"

<flag> has the following meaning:

NE - Negotiate

SS - Session setup

LO - Logoff

TC - Tree connect

TD - Tree disconnect

CR - Create

CL - Close

FL - Flush

RE - Read

WR - Write

LC - Lock

IO - Ioctl

CA - Cancel

EC - Echo

QD - Query directory

CN - Change notify

QI - Query info

SI - Set info

OB - Oplock break

EN - Encrypted packet (in SMB3)

<exp>, <exp-and> and <exp-or> have the following meaning:

– The **<exp>** filter selects flows containing all flags listed in <exp>. To include these flags only, use operator "=".

– The **<exp-and>** is equivalent to <exp>.

– The **<exp-or>** filter selects flows containing at least one of the flags listed in <exp-or>. To include these flags only, use operator "=".

smb2-scmd "<smbopcode2>". Only flows matching **exactly** the specified flags will be processed.

Samba tree structure

- **smb-tree [strcomp] "<string>"** with <string> as a tree structure.

Samba file name

- **smb-file [strcomp] "string"** with <string> as a file name.

Samba file type

- **smb-filetype [=|==|<|>|eq|lt|gt] <value>** where value "1" is a directory and "2" is a file.

Samba file operation type

- **smb-op [=|==|<|>|eq|lt|gt] <sambaoptype>** with <sambaoptype> as a combination of:

0 - Supersede

1 - Open

2 - Create

3 - Overwrite

4 - Open if (Open the file if it already exists; otherwise, create the file.)

5 - Overwrite if (Overwrite the file if it already exists; otherwise, create the file.)

Samba delete flag

- **smb-del [=|==|<|>|eq|lt|gt] <value>** where value "1" indicates file deletion and "0" indicates no deletion.

Samba error flag

- **smb-err [=|==|<|>|eq|lt|gt] <value>** where value "1" indicates error and "0" indicates no error.

SIP Primitives

SIP call ID

sip-callid [<strcomp>] "<str>"

SIP calling party

- **sip-calling [<strcomp>] "<str>"**

SIP called party

- **sip-called [<strcomp>] "<str>"**

SIP VIA

- **sip-via [<strcomp>] "<str>"**

SIP ringing time

- **sip-ringtime [<comp>] <number>**

SIP OK time

- **sip-oktime [<comp>] <number>**

SIP bye time

- **sip-byetime [<comp>] <number>**

SIP RTP IP (IPv4/IPv6)

- **sip-ip <ip>**

SIP RTP audio

- **sip-audio [<comp>] <number>**

SIP RTP video

- **sip-video [<comp>] <number>**

VOIP Packet Type

- **voip-pkttype [<comp>] <number>**

  VOIP packet type list:

  0 - Non-VOIP data

  1 - SIP service requests

  2 - SIP responses on service requests

  3 - SIP call requests

  4 - SIP responses on call requests

8 - RTP voice data

16 - RTCP control and statistical data

RTCP Primitives

RTCP packets count

- **rtcp-pkts [<comp>] <number>**

RTCP octets count

- **rtcp-octets [<comp>] <number>**

RTP jitter

- **rtp-jitter [<comp>] <number>**

RTP jitter is measured in RTP timestamp units. RTP timestamp unit is based on the sampling rate. For example, for the sampling rate of 8000 Hz (PCMA) one unit is equal to 1/8000 of a second. For details, refer to RFC 3550 - interarrival jitter.

RTCP lost packets on client side

- **rtcp-lost [<comp>] <number>**

RTP codec type

- **rtp-codec [<comp>] <number>**

RTCP source count

- **rtcp-sources [<comp>] <number>**

MSSQL Primitives

MSSQL TDS

- **tds-req [<comp>] <number>** - TDS request type
- **tds-ver [<comp>] <number>** - TDS protocol type (<number> should be a 32bit hex number, e.g. 0x71000001)
- **tds-cver [<comp>] <version>** - TDS client version (<version> in format unsigned.unsigned.unsigned)
- **tds-sver [<comp>] <version>** - TDS server version
- **tds-db [<strcomp>] "<str>"** - TDS database context

- **tds-user [<strcomp>] "<str>"** - TDS username
- **tds-host [<strcomp>] "<str>"** - TDS hostname

Filters can be used without parameters to select the elements with valid values.

MSSQL TDS Experimental

- **tds-res [<comp>] <number>** - TDS response type
- **tds-token [<comp>] <number>** - TDS 1st token of response
- **tds-tmr [<comp>] <number>** - TDS transaction manager request type
- **tds-err [<comp>] <number>** - TDS error code
- **tds-envch [<comp>] <number>** - TDS environment change type
- **tds-sql [<strcomp>] "<str>"** - TDS SQL query (search for case-sensitive string)
- **tds-isql [<istrcomp>] "<str>"** - TDS SQL query (search for case-insensitive string)
- **tds-rpc [<strcomp>] "<str>"** - TDS remote procedure name
- **tds-servname [<strcomp>] "<str>"** - TDS server name

Filters can be used without parameters in order to select elements with valid values.

MySQL Primitives

MySQL Protocol Version

- **mysql-ver [<comp>] <number>**

MySQL Server Version

- **mysql-sver [<strcomp>] "<str>"**

MySQL User Authentication Status

- **mysql-auths "<authstr>"**
- **mysql-auths [<comp>] <authnum>**

- with <authnum> - <authstr> as information about successful authentication:

0 - **no**

1 - **yes**

MySQL Username

- **mysql-user [<strcomp>] "<str>"**

MySQL Authentication Method

- **mysql-authm [<strcomp>] "<str>"**

MySQL Database

- **mysql-db [<strcomp>] "<str>"**

MySQL Server and Client Capabilities

- **mysql-cpblts [=] "<flagstring>"**
- **mysql-cpbltc [=] "<flagstring>"** with <flagstring> in following format:

– flagstring ::= "" <flagstringexp> ""

– <flagstringexp> ::= <exp>

– <flagstringexp> ::= <exp-and>

– <flagstringexp> ::= <exp-or>

– <exp> ::= <flag> | <exp><flag>

– <exp-and> ::= <flag> | <exp-and> "&" <flag>

– <exp-or> ::= <flag> | <exp-or> "|" <flag>

– <flag> - "RO" | "VC" | "MO" | "NE" | "TR" | "HE" | "LD" | "AB" | "AP" | "MP" | "MS" | "MQ"

| "NP" | "RD" | "TS" | "IP" | "CY" | "IE" | "41" | "IS" | "LF" | "OD" | "CS" | "NS" | "HD" | "LG" | "RF" | "LP"

<flag> has the following meaning:

RO - Remember Options

VC - SSL Verify Server Certificate

MO - MariaDB: Obsolete (old Client Progress flag)

NE - No EOF Packets (Deprecate EOF)

TR - Session Tracking

HE - Handle Expired Passwords

LD - Length Encoded Client Authentication Data

AB - Connection Attributes

AP - Authentication Plugin (Pluggable Authentication)

MP - Multi Result Set in Prepared Statements

MS - Multi Result Set

MQ - Multiple Queries (Statements)

NP - Native ("Secure") Password Authentication

RD - Reserved (old Client Protocol 4.1 flag)

TS - Transactions

IP - Ignore SIGPIPE

CY - Encryption

IE - Interactive Session

41 - Client Protocol 4.1

IS - Ignore Spaces

LF - Local Files

OD - ODBC support

CS - Compression

NS - No "schema.table.column" Expressions

HD - Handshake (Connect) With Database

LG - Long Flags

RF - Found Rows

LP - Long Password

<exp>, <exp-and> and <exp-or> have the following meaning:

– The **<exp>** filter selects flows containing all flags listed in <exp>. To include these flags only, use operator "=".

– The **<exp-and>** is equivalent to <exp>.

– The **<exp-or>** filter selects flows containing at least one of the flags listed in <exp-or>. To include these flags only, use operator "=".

MySQL Error Code

- **mysql-err [<comp>] <number>**

MySQL Command

- **mysql-cmd [<comp>] <cmdnum>**
- **mysql-cmd "<cmdstr>**"
- with <cmdnum> - <cmdstr> as a combination of:

0 - SLEEP

1 - QUIT

2 - INIT_DB

3 - QUERY

4 - FIELD_LIST

5 - CREATE_DB

6 - DROP_DB

7 - REFRESH

8 - SHUTDOWN

9 - STATISTICS

10 - PROCESS_INFO

11 - CONNECT

12 - PROCESS_KILL

13 - DEBUG

14 - PING

15 - TIME16 - DELAYED_INSERT17 - CHANGE_USER

18 - BINLOG_DUMP

19 - TABLE_DUMP

20 - CONNECT_OUT

21 - REGISTER_SLAVE

22 - STMT_PREPARE

23 - STMT_EXECUTE

24 - STMT_SEND_LONG_DATA

25 - STMT_CLOSE

26 - STMT_RESET

27 - SET_OPTION

28 - STMT_FETCH

29 - DAEMON

30 - BINLOG_DUMP_GTID

31 - RESET_CONNECTION

250 - STMT_BULK_EXECUTE

254 - MULTI

MySQL SQL Query

- **mysql-sql [<strcomp>] "<str>"**

PostgreSQL Primitives

PostgreSQL Protocol Version

- pgsql-ver "**<verstr>**" where **<**verstr**>** should be a string of format "<major>.<minor>" or any prefix thereof, where <major> and <minor> is a numeric value or the ’*’ character. The ’*’ character acts as a wildcard (i.e. matches any value).

PostgreSQL Server Version

- **pgsql-sver "<sverstr>"** Where <sverstr> should be a string of format "<major>.<minor>.<bugfix>" (server versions up to 9.6) or "<major>.<bugfix>" (server versions 10 onwards) or any prefix thereof, where <major>, <minor> and <bugfix> is a numeric value or the '*' character. The '*' character acts as a wildcard (i.e. matches any value, including not present).

> ⓘ **Note**
>
> "<sverstr>" of format "*.1" will match all server versions where minor version is 1 for servers of major version 9 or lower and all server versions where bugfix version is 1 for servers of major version 10 or higher.

PostgreSQL Authentication Method

- pgsql-authm "<authstr>"
- **pgsql-authm [<comp>] <authnum>**
- Where <authstr> and <authnum> are used to specify one of the following authentication methods:

0 - NO AUTHENTICATION

1 - KERBEROS V4

2 - KERBEROS V5

3 - CLEAR PASSWORD

4 - CRYPT PASSWORD

5 - MD5 PASSWORD

6 - SCM CREDENTIALS

7 - GSS

8 - UNKNOWN

9 - SSPI

10 - SASL

PostgreSQL Username

- **pgsql-user [<strcomp>] "<str>"**

PostgreSQL Database

- **pgsql-db [<strcomp>] "<str>"**

PostgreSQL SQLSTATE Error Code

- **pgsql-errc "<sqlstate>"** where <sqlstate> should be an exactly 5 character long string according to the SQLSTATE standard. You may substitute any of its characters for the ’*’ character, which acts as a wildcard (i.e. matches any character).

Note

"pgsql-errc "*****'"" matches any valid error code.

PostgreSQL Error Severity

- **pgsql-errs "<errsstr>"**
- **pgsql-errs [<comp>] <errsnum>**
- Where <errsstr> and <errsnum> are used to specify one of the following error severities:

1 - PANIC

2 - FATAL

3 - ERROR

4 - WARNING

5 - NOTICE

6 - INFO

7 - LOG

8 - DEBUG

254 - UNRECOGNIZED

255 - UNKNOWN

PostgreSQL SQL Query

- **pgsql-sql [<strcomp>] "<str>"**

PostgreSQL Client Message Type

- **pgsql-msgc [=] "<flagstring>"** with <flagstring> in following format:
  - flagstring ::= ’”’ <flagstringexp> ’”’
  - <flagstringexp> ::= <exp>
  - <flagstringexp> ::= <exp-and>
  - <flagstringexp> ::= <exp-or>
  - <exp> ::= <flag> | <exp><flag>
  - <exp-and> ::= <flag> | <exp-and> "&" <flag>
  - <exp-or> ::= <flag> | <exp-or> "|" <flag>
  - <flag> - "?" | "+" | "$" | "#" | "B" | "C" | "D" | "E" | "H" | "F" | "P" | "p" | "Q" | "S" | "X" |"r" | "h" | "d" | "c" | "f"

<flag> has the following meaning:

? - Unknown message

+ - Startup message

$ - SSL request

- Cancel request

B - Bind

C - Close

D - Describe

E - Execute

H - Flush

F - Function call

P - Parse

p - Password message

Q - Query

S - Sync

X - Terminate

r - Standby status update

h - Hot standby feedback

d - Copy data

c - Copy done

f - Copy fail

<exp>, <exp-and> and <exp-or> have the following meaning:

- The **<exp>** filter selects flows containing all flags listed in <exp>. To include these flags only, use operator "=".
- The **<exp-and>** is equivalent to <exp>.
- The **<exp-or>** filter selects flows containing at least one of the flags listed in <exp-or>. To include these flags only, use operator "=".

PostgreSQL Server Message Type

- **pgsql-msgs [=] "<flagstring>"** with <flagstring> in following format:
  - flagstring ::= ”” <flagstringexp> ””
  - <flagstringexp> ::= <exp>
  - <flagstringexp> ::= <exp-and>
  - <flagstringexp> ::= <exp-or>
  - <exp> ::= <flag> | <exp><flag>
  - <exp-and> ::= <flag> | <exp-and> "&" <flag>
  - <exp-or> ::= <flag> | <exp-or> "|" <flag>

  - <flag> - "?" | "R" | "K" | "2" | "3" | "C" | "G" | "H" | "W" | "D" | "I" | "E" | "V" | "n" | "N" |"A" | "t" | "S" | "1" | "s" | "Z" | "T" | "w" | "k" | "$" | "%" | "d" | "c"

<flag> has the following meaning:

? - Unknown message

R - Authentication

K - Backend key data

2 - Bind complete

3 - Close complete

C - Command complete

G - Copy in response

H - Copy out response

W - Copy both response

D - Data row

I - Empty query response

E - Error response

V - Function call response

n - No data

N - Notice response

A - Notification response

t - Parameter description

S - Parameter status

1 - Parse complete

s - Portal suspended

Z - Ready for query

T - Row description

w - Xlog data

k - Primary keepalive

$ - SSL accept

% - SSL deny

d - Copy data

c - Copy done

<exp>, <exp-and> and <exp-or> have the following meaning:

- The **<exp>** filter selects flows containing all flags listed in <exp>. To include these flags only, use operator "=".
- The **<exp-and>** is equivalent to <exp>.

- The **<exp-or>** filter selects flows containing at least one of the flags listed in <exp-or>. To include these flags only, use operator "=".

RADIUS Primitives

RADIUS Username

- **radius-login [comp] "<string>"**

RADIUS Calling Station ID

- **radius-calling-station-id [comp] "<string>"**

RADIUS Called Station ID

- **radius-called-station-id [comp] "<string>"**

RADIUS NAT IP address

- **radius-nat-address [comp] <ipaddr>**

RADIUS NAT port start

- **radius-port-start [comp] <number>**

RADIUS NAT port end

- **radius-port-end [comp] <number>**

TLS Primitives

TLS Content type

- **tls-cont [flcomp] "<flagtokens>"** where <flagtokens> is list of tokens representing desired flags. These are valid TLS content type flags:
- **CCS** - Content type CCS
- **ALERT** - Content type ALERT
- **HS** - Content type HANDSHAKE
- **DATA** - Content type APP DATA

The tokens in <flagtokens> can be joined by either ’&’ (all specified flags are set) or ’|’ (at least one of specified flags is set). Combination of ’&’ and ’|’ in one filter is not permitted.

TLS Handshake type

- **tls-hshk [flcomp] "<flagtokens>"** where <flagtokens> is list of tokens representing desired flags. These are valid TLS handshake type flags:
- **HR** - Hello request
- **CH** - Client hello
- **SH** - Server hello
- **HVER** - Hello verify request
- **NST** - New session ticket
- **EED** - End of early data
- **HRET** - Hello retry request
- **ENC** - Encrypted extensions
- **CER** - Certificate
- **KSRV** - Server key exchange
- **CRQ** - Certificate request
- **SHD** - Server hello done
- **CVER** - Certificate verify
- **KCL** - Client key exchange
- **FIN** - Finished
- **CURL** - Certificate url
- **CST** - Certificate status
- **SUPL** - Supplemental data
- **KUPD** - Key update
- **MSGH** - Message hash
- **UNKN** - Unknown

The tokens in <flagtokens> can be joined by either ’&’ (all specified flags are set) or ’|’ (at least one of specified flags is set). Combination of ’&’ and ’|’ in one filter is not permitted.

TLS Setup time

- **tls-setup [comp] <time-milli>**

TLS Server version

- **tls-sver [comp] "<string>"**
- **tls-sver [comp] <number>**

Argument can be either numeric representation of tls version or its text name. Numeric value can be hexadecimal (prefixed with "0x") or decimal. Supported TLS versions are "SSL 2.0", "SSL 3.0", "TLS 1.0", "TLS 1.1" and "TLS 1.2". Hexadecimal values are 0x002, 0x0300, 0x0301, 0x0302 and 0x0303 in respective order.

TLS Server random ID

- **tls-srnd "<bytes>"**

<bytes> is some part of random ID byte sequence (entered as hexadecimal digits). One hexadecimal digit corresponds to one nibble (4bits). For example filter tls-srnd "90a0b0" will match all flows in which TLS Server random ID contains sequence of 3 bytes 0x90 0xa0 0xb0 or sequence of 4 bytes 0x*9 0x0a 0x0b 0x0*, where "*" is any nibble.

TLS Server session ID

- **tls-ssid [comp] <number>**

<bytes> is some part of session ID byte sequence (entered as hexadecimal digits). One hexadecimal digit corresponds to one nibble (4bits). For example filter tls-ssid "90a0b0" will match all flows in which TLS Server session ID contains sequence of 3 bytes 0x90 0xa0 0xb0 or sequence of 4 bytes 0x*9 0x0a 0x0b 0x0*, where "*" is any nibble.

TLS Cipher suite

- **tls-ciph "<bytes>"**
- **tls-ciph [=] "<string>"**

TLS Application layer protocol negotiation

- **tls-alpn [strcomp] "<string>"**

TLS Server name indication

- **tls-sni [strcomp] "<string>"**

TLS Server name length

- **tls-snlen [comp] <number>**

TLS server compression method

- **tls-sscm [comp] <number>**
- **tls-sscm [comp] <method>**

With <number> and <method> as one of these:

- **0** - NULL
- **1** - DEFLATE
- **64** - LZS

TLS Client version

- **tls-cver [comp] "<string>"**
- **tls-cver [comp] <number>**

Argument can be either numeric representation of tls version or its text name. Numeric value can be hexadecimal (prefixed with "0x") or decimal. Supported TLS versions are "SSL 2.0", "SSL 3.0", "TLS 1.0", "TLS 1.1" and "TLS 1.2". Hexadecimal values are 0x002, 0x0300, 0x0301, 0x0302 and 0x0303 in respective order.

TLS Cipher suites and Elliptic curves

- **tls-ciphs [=] "<tokens>"**
- **tls-ciphse [=] "<tokens>"** - exact order match
- **tls-ece [=] "<tokens>"** - exact order match
- **tls-ec [=] "<tokens>"**

<tokens> is comma separated list of either cipher suite / elliptic curve text names or their hexadecimal representations. Combination is not allowed, so all values in the list will be treated either as hexadecimal numbers or text. Filters will match only if all values are found inside record. Exact order filters will match only if sequence of values is found inside record array in specified order. Exact filter (optional equal sign is used) will match only if there are no other values in record array than those specified. Hexadecimal representation of one cipher suite has form 0xAAAA. Cipher suite / elliptic curve is represented as two-byte number, so maximum number of digits is four. For text tokens, there are no input rules. Partial text names are also allowed (substring compare method is used).

TLS Client random ID and Client session ID

- **tls-crnd "<bytes>"**
- **tls-csid "<bytes>"**

<bytes> is some part of random ID / session ID byte sequence (entered as hexadecimal digits). One hexadecimal digit corresponds to one nibble (4bits).

TLS Extensions

- **tls-ext [=] "<tokens>"** - Extension types
- **tls-exte [=] "<tokens>"** - Extension types (exact order)
- **tls-exl [=] "<tokens>"** - Extension lengths
- **tls-exle [=] "<tokens>"** - Extension lengths (exact order)

<tokens> is comma separated list of decimal values. Filters will match only if all values are found inside record. Exact order filters will match only if sequence of values is found inside record array in specified order. Exact filter (optional equal sign is used) will match only if there are no other values in record array than those specified. Extension type and extension length is represented as two-byte number, so maximum allowed value is 65535.

TLS Elliptic curves point formats

- **tls-ecpf "<tokens>"**

<tokens> is comma separated list of either decimal or text values. Maximum allowed decimal number is 254. For text values, only full text names are allowed. Numeric and text tokens may be combined. Recognized names are "uncompressed" (0), "ansiX962_compressed_prime" (1) and "ansiX962_compressed_char2" (2).

TLS Client key length

- **tls-cklen [comp] <number>**

TLS Certificate

- **tls-icn [strcomp] "<string>"** - Certificate issuer common name
- **tls-scn [strcomp] "<string>"** - Subject common name
- **tls-son [strcomp] "<string>"** - Subject organisation name. Comparison is case insensitive.
- **tls-vfrom [comp] <timestamp>** - Certificate validity since
- **tls-vfrom [comp] "<date>"** - Certificate validity since
- **tls-vto [comp] <timestamp>** - Certificate validity until
- **tls-vto [comp] "<date>"** - Certificate validity until <date> is text specification of date/time in format "YYYY-MM-DD HH:MM:SS". <timestamp> is date/time represented seconds since epoch. Special value "now" is also accepted and interprets as current time.
- **tls-salg "<algorithm name>"** - Signature algorithm
- **tls-pkalg "<algorithm name>"** - Public key algorithm
- **tls-pklen [comp] <number>** - Public key length
- **tls-snum "<bytes>"** - TLS certificate serial number. <bytes> is a part of the TLS certificate serial number (entered as hexadecimal digits). One hexadecimal digit corresponds to one nibble (4bits).
- **tls-san [strcomp] "<string>"** - TLS certificate subject alternate names

TLS JA3 Fingerprint

- **tls-ja3 "<bytes>"** <bytes> is some part of JA3 Fingerprint byte sequence (entered as hexadecimal digits). One hexadecimal digit corresponds to one nibble (4bits).

VxLAN Primitives

VxLAN VNI

- **vxlan-vni [comp] <number>**

IEC104

- **iec104-pktlen [comp] <number>** - IEC104 Packet Length
- **iec104-fmt [strcomp] "<fmtstr>"** - IEC104 Frame Format with <fmtstr> as one of these characters:
    - **I** - I-frame
    - **S** - S-frame
    - **U** - U-frame
- **iec104-asdu-type [comp] <number>** - IEC104 ASDU Type
- **iec104-asdu-objcount [comp] <number>** - IEC104 ASDU Object Count
- **iec104-asdu-cot [comp] <number>** - IEC104 ASDU Cause Of Transmission
- **iec104-asdu-org [comp] <number>** - IEC104 ASDU Originator Address
- **iec104-asdu-addr [comp] <number>** - IEC104 Common ASDU Address

CoAP

- **coap-ver [comp] <number>**
- **coap-mid [comp] <number>**
- **coap-code [strcomp] "<str>"** - with <str> as a number in format "0.00"
- **coap-opcount [comp] <number>**
- **coap-type "<str>"** - with <str> as one of these:
  - **CNF** - Confirmable message
  - **NCNF** - Nonconfirmable message
  - **ACK** - Acknowledge
  - **RST** - Reset
- **coap-accept [comp] <number>**
- **coap-contentfmt [comp] <number>**
- **coap-token [strcomp] "<str>"** - hexadecimal representation of bytestream (maximal length 16 characters). Example: coap-token = "b38a4e20"
- **coap-uripath [strcomp] "<str>"**
- **coap-uriquery [strcomp] "<str>"**
- **coap-urihost [strcomp] "<str>"**

GOOSE

- goose-appid [comp] <number>
- goose-cbref [strcomp] "<str>"
- goose-dataset [strcomp] "<str>"
- goose-id [strcomp] "<str>"
- goose-stnum [comp] <number>

MMS

- mms-type [comp] <number> - with <number> as one of these:
  - 0 - confirmed-Request
  - 1 - confirmed-Response
  - 2 - confirmed-Error
  - 3 - unconfirmed
  - 4 - reject
  - 5 - cancel-Request
  - 6 - cancel-Response
  - 7 - cancel-Error
  - 8 - initiate-Request
  - 9 - initiate-Response
  - 10 - initiate-Error
  - 11 - conclude-Request
  - 12 - conclude-Response
  - 13 - conclude-Error
- mms-conf-service-req [comp] <number>
- mms-conf-service-resp [comp] <number> -with <number> for mms-conf-service-req and mms-conf-service-resp as one of these:

    - 0 - status
    - 1 - getNameList
    - 2 - identify
    - 3 - rename
    - 4 - read
    - 5 - write
    - 6 - getVariableAccessAttributes
    - 7 - defineNamedVariable
    - 8 - defineScatteredAccess
    - 9 - getScatteredAccessAttributes
    - 10 - deleteVariableAccess
    - 11 - defineNamedVariableList
    - 12 - getNamedVariableListAttributes
    - 13 - deleteNamedVariableList
    - 14 - defineNamedType
    - 15 - getNamedTypeAttributes
    - 16 - deleteNamedType

- 17 - input
- 18 - output
- 19 - takeControl
- 20 - relinquishControl
- 21 - defineSemaphore
- 22 - deleteSemaphore
- 23 - reportSemaphoreStatus
- 24 - reportPoolSemaphoreStatus
- 25 - reportSemaphoreEntryStatus
- 26 - initiateDownloadSequence
- 27 - downloadSegment
- 28 - terminateDownloadSequence
- 29 - initiateUploadSequence
- 30 - uploadSegment
- 31 - terminateUploadSequence
- 32 - requestDomainDownload
- 33 - requestDomainUpload
- 34 - loadDomainContent
- 35 - storeDomainContent
- 36 - deleteDomain
- 37 - getDomainAttributes
- 38 - createProgramInvocation
- 39 - deleteProgramInvocation
- 40 - start
- 41 - stop
- 42 - resume
- 43 - reset
- 44 - kill
- 45 - getProgramInvocationAttributes
- 46 - obtainFile
- 47 - defineEventCondition
- 48 - deleteEventCondition
- 49 - getEventConditionAttributes

- 50 - reportEventConditionStatus
- 51 - alterEventConditionMonitoring

- 52 - triggerEvent
- 53 - defineEventAction
- 54 - deleteEventAction
- 55 - getEventActionAttributes
- 56 - reportEventActionStatus
- 57 - defineEventEnrollment
- 58 - deleteEventEnrollment
- 59 - alterEventEnrollment
- 60 - reportEventEnrollmentStatus
- 61 - getEventEnrollmentAttributes
- 62 - acknowledgeEventNotification
- 63 - getAlarmSummary
- 64 - getAlarmEnrollmentSummary
- 65 - readJournal
- 66 - writeJournal
- 67 - initializeJournal
- 68 - reportJournalStatus
- 69 - createJournal
- 70 - deleteJournal
- 71 - getCapabilityList
- 72 - fileOpen
- 73 - fileRead
- 74 - fileClose
- 75 - fileRename
- 76 - fileDelete
- 77 - fileDirectory
- 78 - additionalService

- 80 - getDataExchangeAttributes
- 81 - exchangeData
- 82 - defineAccessControlList
- 83 - getAccessControlListAttributes
- 84 - reportAccessControlledObjects
- 85 - deleteAccessControlList
- 86 - changeAccessControl
- 87 - reconfigureProgramInvocation - only for mss-conf-service-resp

- mms-unconf-service [comp] <number> - with <number> as one of these:
  - 0 - informationReport
  - 1 - unsolicitedStatus
  - 2 - eventNotification

DLMS

- **dlms-type [comp] <number>** - with <number> as one of these:
  - 192 - get-request
  - 193 - set-request

  - 194 - event-notification-request
  - 195 - action-request
  - 196 - get-response
  - 197 - set-response
  - 199 - action-response
- **dlms-subtype [comp] <number>**
  - 3073 (0xc001) - get-request-normal
  - 3074 (0xc002) - get-request-next
  - 3075 (0xc003) - get-request-with-list
  - 49409 (0xc101) - set-request-normal
  - 49410 (0xc102) - set-request-with-first-data-block
  - 49411 (0xc103) - set-request-with-datablock
  - 49412 (0xc104) - set-request-with-list
  - 49413 (0xc105) - set-request-with-list-and-first-data-block
  - 49921 (0xc301) - action-request-normal
  - 49922 (0xc302) - action-request-next-pblock
  - 49923 (0xc303) - action-request-with-list
  - 49924 (0xc304) - action-request-with-first-pblock
  - 49925 (0xc305) - action-request-with-list-and-first-pblock
  - 49926 (0xc306) - action-request-with-pblock
  - 50177 (0xc401) - get-response-normal
  - 50178 (0xc402) - get-response-with-datablock
  - 50179 (0xc403) - get-response-with-list
  - 50433 (0xc501) - set-response-normal
  - 50434 (0xc502) - set-response-datablock
  - 50435 (0xc503) - set-response-last-data-block
  - 50436 (0xc504) - set-response-last-data-block-with-list
  - 50437 (0xc505) - set-response-with-list
  - 50945 (0xc701) - action-response-normal
  - 50946 (0xc702) - action-response-with-pblock
  - 50947 (0xc703) - action-response-with-list
  - 50948 (0xc704) - action-response-next-pblock

- **dlms-classid [comp] <number>**
- **dlms-obis [arraycomp] <obidnum>** Where <obidnum> is ID consisting of 6 digits delimited with . (dot), each digit has maximal size of one byte, arraycomp is array comparator, only = (array exact equality) is supported. Example: dlms-obis = 1.0.99.1.0.255 To filter group of ID’s use common prefix terminated with character ’.’ (dot) Example: "dlms-obis 1.0.99." filters all ID’s with the first 3 digits same, last 3 digits are treated as don’t care.
- **dlms-attr-method-id [comp] <number>**
- **dlms-data-type [comp] <number>** - with <number> as one of these:

-
  - 0 - null-data
  - 1 - array
  - 2 - structure
  - 3 - boolean
  - 4 - bit-string
  - 5 - double-long
  - 6 - double-long-unsigned
  - 9 - octet-string
  - 10 - visible-string
  - 13 - bcd

  - 15 - integer
  - 16 - long
  - 17 - unsigned
  - 18 - long-unsigned
  - 19 - compact-array
  - 20 - long64
  - 21 - long64-unsigned
  - 22 - enum
  - 23 - float32
  - 24 - float64
  - 25 - date-time
  - 26 - date
  - 27 - time
  - **dlms-data-length [comp] <number>**

- **dlms-data-access-result [comp] <number>** - with <number> as one of these:

- 0 - success
- 1 - hardware-fault
- 2 - temporary-failure
- 3 - read-write-denied
- 4 - object-undefined
- 9 - object-class-inconsistent
- 11 - object-unavailable
- 12 - type-unmatched
- 13 - scope-of-access-violated
- 14 - data-block-unavailable
- 15 - long-get-aborted
- 16 - no-long-get-in-progress
- 17 - long-set-aborted
- 18 - no-long-set-in-progres
- 250 - other-reason

- **dlms-action-result [comp] <number>** - with <number> as one of these:
  - 0 - success
  - 1 - hardware-fault
  - 2 - temporary-failure
  - 3 - read-write-denied
  - 4 - object-undefined
  - 9 - object-class-inconsistent
  - 11 - object-unavailable
  - 12 - type-unmatched
  - 13 - scope-of-access-violated
  - 14 - data-block-unavailable
  - 15 - long-action-aborted
  - 16 - no-long-action-in-progress
  - 250 - other-reason

VMware NSX fields

- **nsx-ruleid <number>** - Firewall rule ID
- **nsx-vnicindex <number>** - VNIC index
- **nsx-vmuuid <number> [<number>]** - filters flow records with specific VM UUID that uniquely identifies the VM. This ID comprises of two hexadecimal numbers. You can provide just the first one or both. Each hexa number must be preceded with 0x prefix. This is an example for VM UUID (00 11 22 33 44 55 66 77-88 99 aa bb cc dd ee ff): "nsx-vmuuid 0x0011223344556677" or "nsx-vmuuid 0x0011223344556677 0x8899aabbc-cddeeff".
- **nsx-vmuuid-mac <addr>** - since VM UUID usually contains MAC address in its first part, you can use MAC in a filter as well. It will be matched with the first VMUUID number. This is an example how to filter out the machine with mac address 00:11:22:33:44:55: "nsx-vmuuid-mac 00:11:22:33:44:55".

Network Performance Metrics Primitives

- **npm-rtt [[<comp>] <realnumber>]** - Round Trip Time (RTT)
- **npm-srt [[<comp>] <realnumber>]** - Server Response Time (SRT)
- **npm-retr [[<comp>] <realnumber>]** - Packet Retransmissions (RTR)
- **npm-ooo [[<comp>] <realnumber>]** - Number of Out of Order packets (OoO)
- **npm-jdev [[<comp>] <realnumber>]** - Standard Deviation of Jitter (SDV Jitter)
- **npm-javg [[<comp>] <realnumber>]** - Average Jitter (AVG Jitter)
- **npm-jmin [[<comp>] <realnumber>]** - Minimal Jitter (MIN Jitter)
- **npm-jmax [[<comp>] <realnumber>]** - Maximal Jitter (MAX Jitter)
- **npm-ddev [[<comp>] <realnumber>]** - Standard Deviation of Inter-packet Delay (SDV IPD)
- **npm-davg [[<comp>] <realnumber>]** - Average Inter-packet Delay (AVG IPD)
- **npm-dmin [[<comp>] <realnumber>]** - Minimal Inter-packet Delay (MIN IPD)
- **npm-dmax [[<comp>] <realnumber>]** - Maximal Inter-packet Delay (MAX IPD)

with <realnumber> as a real number in format NNN.nnn.

Cisco Primitives

Cisco AVC - ART

- **art-snt [[<comp>] <realnumber>]** - Sum Server Network Time (Sum SNT)
- **art-sntmin [[<comp>] <realnumber>]** - Minimal Server Network Time (MIN SNT)
- **art-sntmax [[<comp>] <realnumber>]** - Maximal Server Network Time (MAX SNT)
- **art-cnt [[<comp>] <realnumber>]** - Sum Client Network Time (Sum CNT)
- **art-cntmin [[<comp>] <realnumber>]** - Minimal Client Network Time (MIN CNT)
- **art-cntmax [[<comp>] <realnumber>]** - Maximal Client Network Time (MAX CNT)
- **art-srt [[<comp>] <realnumber>]** - Sum Server Response Time (Sum SRT)
- **art-srtmin [[<comp>] <realnumber>]** - Minimal Server Response Time (MIN SRT)
- **art-srtmax [[<comp>] <realnumber>]** - Maximal Server Response Time (MAX SRT)

Cisco NEL

- **nat event <add|delete>**
- **nat event [<comp>] <number>**
- [**src**|**dst**] **nip <ip>** - selects the NAT IP address.

- [**src**|**dst**] **nport <port>** - selects the NAT port.
- **ingress vrf <number>** - selects the vrf .

Cisco NSEL/ASA

- **asa event <ignore|create|term|delete|deny>**
- **asa event [<comp>] <number>**
- **asa event denied <ingress|egress|interface|nosyn>**
- **asa xevent [<comp>] <number>**
- [**src**|**dst**] **xip <ip>** - selects the translated IP address.
- [**src**|**dst**] **xport <port>** - selects the translated port.
- **ingress <ACN|ACE|XACE> [<comp>] <number>** - selects/compares an ingress ACL ID fields.
- **egress <ACN|ACE|XACE> [<comp>] <number>** - selects/compares an egress ACL ID fields.

Aggregated Flows Primitives

- **flows [<comp>] <num> [<scale>]**- filters out NetFlow records with a specific number of aggregated flows.

<scale> is a scaling factor. Allowed prefixes are (Kilo) **k**, (Mega) **m**, (Giga) **g**, (Tera) **t**. The factor is 1024.

Packets, Bytes and Bits Primitives

Packets

- **packets [<comp>] <num>** - filters out netflow records with a specific packet count.

  Example: packets > 1k.

Bytes

- **bytes [<comp>] <num>** - filters out netflow records with a specific byte count.

  Example: bytes 46.

Packets per second

- **pps [<comp>] <num>** - specifies the pps of the flow.[<scale>]

Bits per second

- **bps [<comp>] <num>** - specifies the bps of the flow.[<scale>]

Bytes per packet

- **bpp [<comp>] <num>** - specifies the bpp of the flow.[<scale>]

Packets, Bytes and Bits examples

- **packets > 1 M and bytes < 1700 M** - matches records with more than 1 mega packets, but under 1700 MB.
- **(pps > 200 K or bps > 180 M) and bpp < 130** - matches records with minimal threshold of at least 200 K packets per second or 180 M bits per second) while keeping packets under 130 B.
- **bpp > 1500 and bytes > 100 M** - finds jumbo packets flows larger than 100 MB.

Duration Primitives

Duration

- **duration [<comp>] <num>** - specifies the duration in milliseconds.

Duration examples

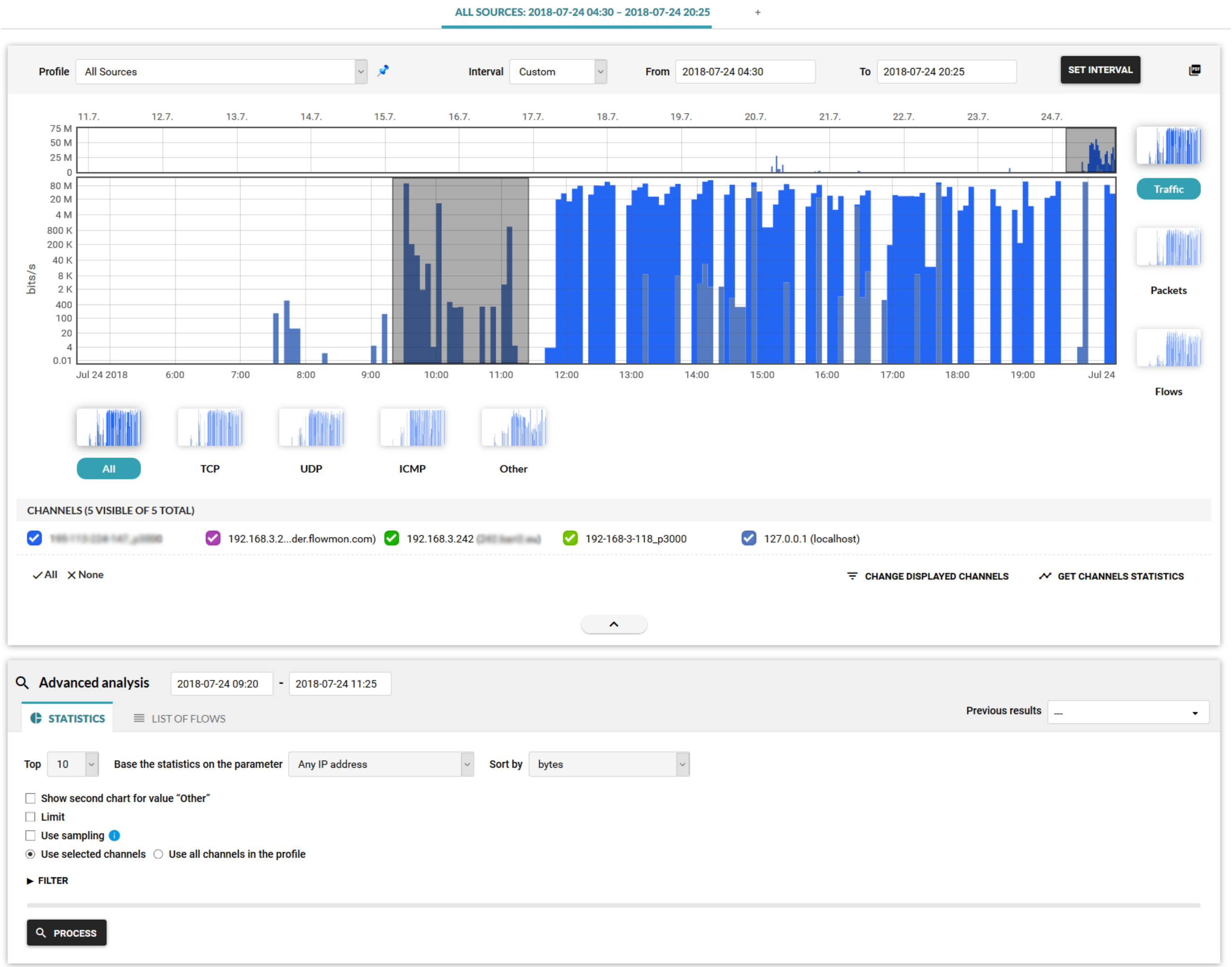
- **duration > 1000 and duration < 5000** - matches flow records which took between 1 and 5 seconds.

Other Filter Examples

- **proto tcp and net 192.168/16 and src port >> 1024 and dst port 80 and bytes > 2048** - matches HTTP/TCP communication in internal network larger than 2048 bytes.
- **proto tcp and (net 192.168/16) and (src port > 1024 and dst port 80) and (bytes > 2048)** - is identical to the previous (with added brackets for readability).

Analysis

Detailed analysis of flow data can be performed on the **Analysis** page.



Profile: All Sources

Interval: Custom

From: 2018-07-24 04:30

To: 2018-07-24 20:25

SET INTERVAL

CHANNELS (5 VISIBLE OF 5 TOTAL)

☑ [redacted] ☑ 192.168.3.2...der.flowmon.com) ☑ 192.168.3.242 [redacted] ☑ 192-168-3-118_p3000 ☑ 127.0.0.1 (localhost)

✓All ✕None

CHANGE DISPLAYED CHANNELS

GET CHANNELS STATISTICS

Advanced analysis 2018-07-24 09:20 - 2018-07-24 11:25

STATISTICS LIST OF FLOWS

Previous results: —

Top: 10 Base the statistics on the parameter: Any IP address Sort by: bytes

□ Show second chart for value "Other"

□ Limit

□ Use sampling

● Use selected channels ○ Use all channels in the profile

▸ FILTER

PROCESS

Monitored traffic analysis panel

The page is divided into three parts: The upper part serves for viewing flow data and for selecting of a time slot or window. The middle part shows a graph legend and allows to switch the particular channels and NPM (network performance metrics) on and off.

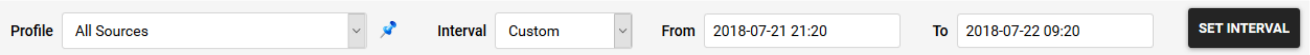
The button **Change displayed channels** opens a selection form for adding and removing channels from graph and legend. Checkbox **Show new channels automatically** in this form enables automatic addition of new channels (for example newly detected flow sources will be automatically added into the All Sources graph). Checkbox **Show NPM statistics** will add into the detailed graph new y axis and three new line graphs for following network performance metrics provided by Flowmon Probes: Traffic Jitter, Round Trip Time and Server response time.

The button **Get channels statistics** opens a table containing information about the selected time window.

You can choose from charts displaying number of flows (**Flows**), number of packets (**Packets**) and number of transferred bits (**Traffic**). When you click on one of the small charts, it is swapped with the main chart. You can choose the best suitable chart for your situation / investigation.

In addition for profiles version 1, data can be filtered according to the network protocols - **All**, **TCP**, **UDP**, **ICMP**, **Other**. Note, **All** means all data without filtering and **Other** means protocols other than TCP, UDP and ICMP. This feature is not available for 1-min and 30-sec profiles.

Time slot shown in the charts can be set either using the **Interval** combo box above the charts or by manual setting of start (**From**) and end (**To**) time next to the combo box. If you set the range manually, you must confirm your choice by clicking the **Set Interval** button. Minimum time interval is 6 hours.



Profile and time interval selection panel

Change of Time Slot

Time slots are five minutes long, 1 minute long or 30 seconds long (depends on their type). They always start at 5 minutes (e.g. 12:00, 12:05, 12:10, 12:15), 1 minutes or 30 seconds (e.g. 12:00:00, 12:02:03) respectively. Time window consists of more neighboring time slots. After entering the **Analysis** page, the charts display the last 12 hours. The time cursor is at the position of the last time slot. Selected time slot or time window and profile name is always displayed in the title of the tab. The time window can be changed by the following ways:

- By clicking a single time slot in the chart. This moves the time cursor to the selected position.
- By dragging the cursor in the chart using left mouse button. This selects a time window. Selected time window can be later adjusted by dragging its center of edges.

The charts and statistics table automatically update after selecting a new time slot and they respect the following limitation: When moving the cursor to the area with expired (and deleted) data, the statistics are calculated from inaccurate RRD data. This area is differentiated by the gray background in the left part of the chart and when RRD data is used, the statistics table displays a warning about inaccuracy of data.

Overview Chart

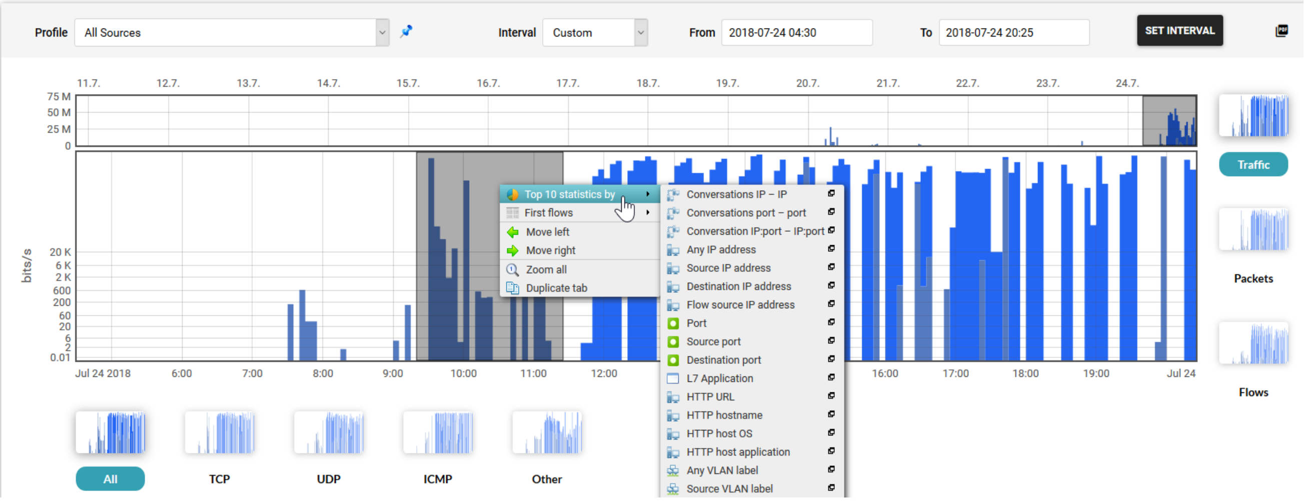
Above the main chart there is an overview chart which makes orientation in the detailed chart easier even at higher zoom levels. The data range of the overview chart is set up automatically and the detailed chart always displays the selected area of the overview chart.

Dragging selection or changing selection size of the overview chart causes loading of corresponding data to the detailed chart and changing the values in the fields **From** and **To** at the top of the page. Also moving of detailed chart left or right moves the selection in the overview chart.

Context Menu

When clicking the right mouse button above the chart area, the context menu pops up. This menu allows to make common queries over the selected time window and control the chart. Available statistics correspond to the items in the filter at the bottom of the page and their meaning will be described later.

There is an option to Duplicate tab with the symbol of two windows. The same effect can be achieved by clicking the plus symbol on the rightmost tab.



Profile All Sources

Interval Custom

From 2018-07-24 04:30

To 2018-07-24 20:25

Context menu

Chart Settings

The charts can be displayed in several modes depending on requested details. After hovering the zooming buttons at the bottom right corner of the chart, a floating menu appears. This menu allows to change the chart settings. **Logarithmic axis Y** switches between linear and logarithmic scale of the chart. Data can be displayed either as a line chart or as a stacked chart (**Stacked chart**).

The stacked chart composes the channels at each other, line chart display them independently. Line chart is suitable for finding peeks, stacked chart is better when viewing a summary. The rest of options controls the chart scale and zooming.

Advanced Analysis of Selected Data

Once flow data is chosen for analysis, it is possible to apply requested filter on it using the form at the bottom of the page.

To select data for analysis, you need to select time interval in the Detailed chart and you can also choose some of the channels in the graph. If you select **Use all channels in profile** option, than all channels of profile will be processed (including hidden channels disabled in **Change displayed channels** form). If you select **Use selected channels** option then only channels displayed in the detailed graph will be processed.

To enter user filter string, click the **Filter** link which expands the field for the query. The syntax corresponds the syntax of nfdump commands and its basics are described below.

Press the **Process** button.

Named Filters

Often used filters can be saved and used repeatedly. Such filter can be created by the following was: Enter the filter to the text area and click the **Save filter** button. Enter the filter name and confirm it by clicking OK button. Saved filter can be found in My filters combo box under the filter field. Named filter can be whenever modified or deleted using corresponding buttons next to the filter name in the combo box.

Types of Analysis

Recorded NetFlow data can be processed by two ways: Either it is possible to use NetFlow statistics (**Statistics** tab) or it is possible to work with the list of particular flows (**List of flows** tab). Each tab has different configuration options.

Statistics (TopN)

The options description:

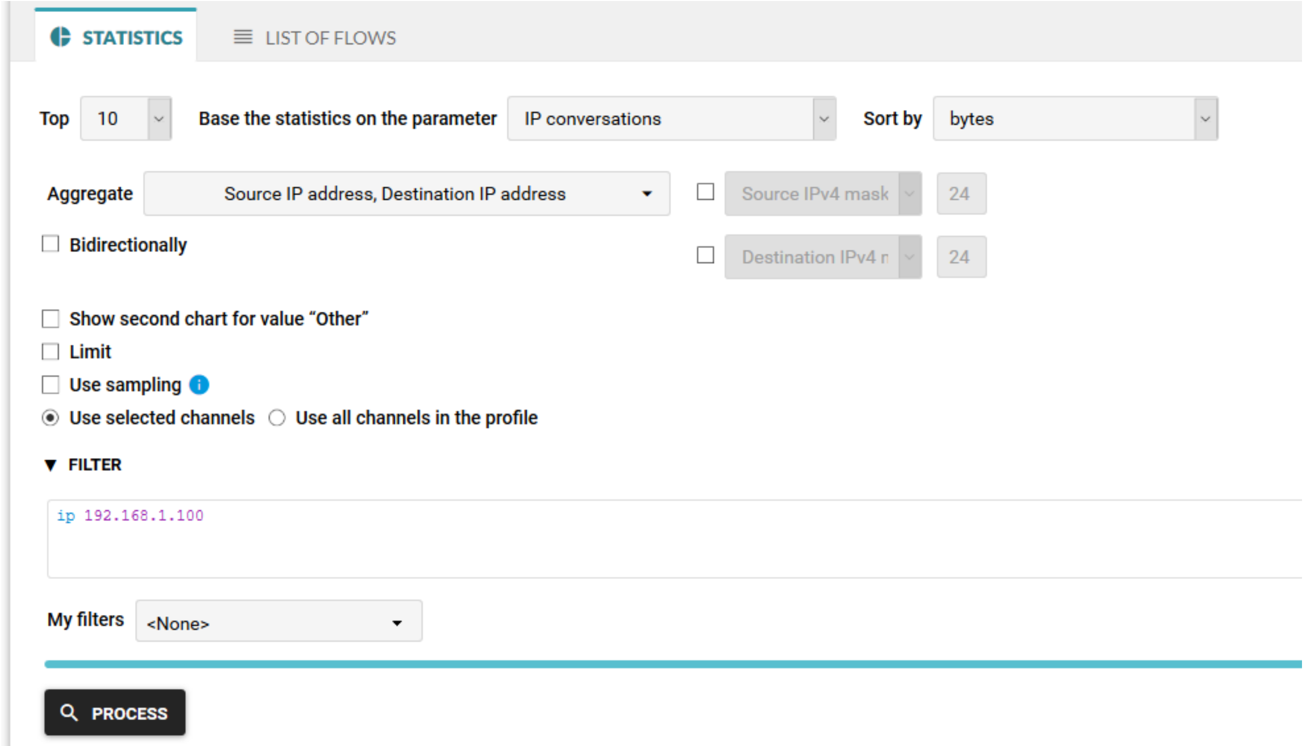
- **Top** - Limit the statistics to the first top N
- **Statistics by** - Select the statistics you want from the menu and the order option
- **Limit** - Limit the output only to those statistic lines whose packets or bytes match the specified limit.
- **Use sampling** - Use this option if you want to process a big amount of data. It will sample the flows in database in 1:10 ratio in order to speed up the computation in exchange for lesser accuracy..

Once the statistics results are displayed new option becomes available:

- **Show in time** - Once the statistics results are displayed, you can show in time graph the first 20 rows in table.

Note

Processing of NetFlow data is a demanding task. If you work with a large network, the processing can take very long time, especially when you choose a big time window and more sources.



Top 10 Base the statistics on the parameter IP conversations Sort by bytes

Aggregate Source IP address, Destination IP address □ Source IPv4 mask 24

□ Bidirectionally □ Destination IPv4 r 24

□ Show second chart for value "Other"
□ Limit
□ Use sampling
● Use selected channels ○ Use all channels in the profile

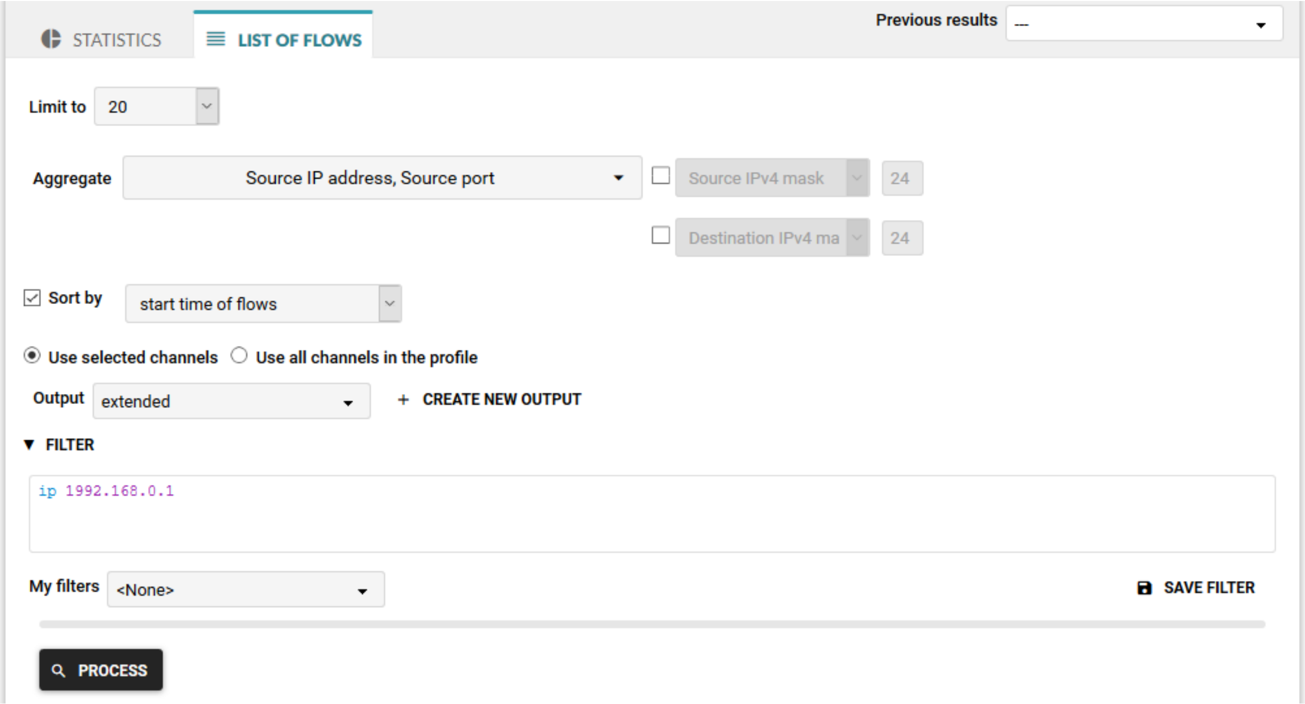
▼ FILTER

```
ip 192.168.1.100
```

My filters <None>

Statistics (TopN) panel

List of Flows



Limit to 20

Aggregate Source IP address, Source port

□ Source IPv4 mask 24

□ Destination IPv4 ma 24

☑ Sort by start time of flows

● Use selected channels ○ Use all channels in the profile

Output extended

```
ip 1992.168.0.1
```

My filters <None>

List of flows panel

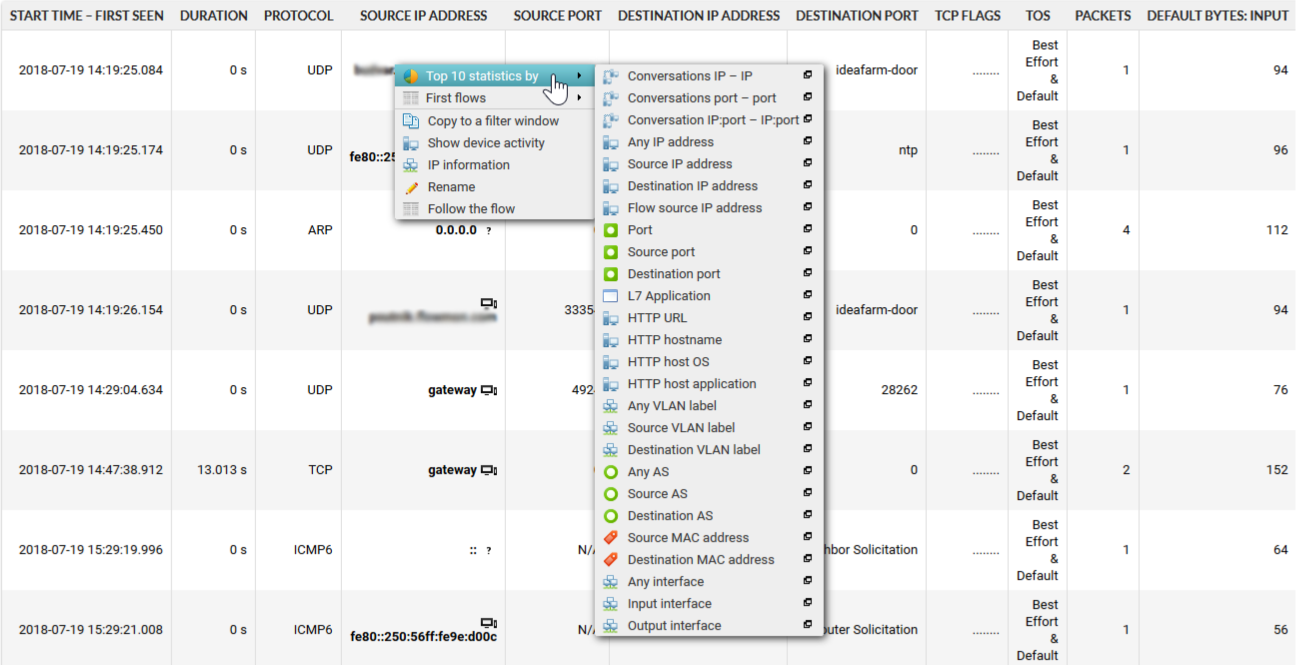
Description of options:

- **Limit to** - List only the first N flows of the selected time slot.
- **Aggregate** - Option to aggregate the flows. By clicking on the checkboxes, you can select how you want to have your flows aggregated. You may also aggregate entire subnets when selecting srcIPv4/<subnet bits> By default the flows are not aggregated.
- **Sort by** - When listing flows from different channels/sources you may sort them according the start time of the flows. Otherwise the flows are listed in sequence of the selected channels.
- **Output** - Allows to change the output format. It is possible to use predefined formats **line**, **long** and **extended** or define a custom one.
  - **Line** - displays one NetFlow record per line (if aggregation is off).
  - **Long** - this format displays extended information like TCP flags, Type of Service etc.
  - **Extended** this format extends information provided by long format. In addition it contains items pps (number of packets per second), bps (number of bytes per second) and bpp (bytes per packet).

Besides these predefined formats it is possible to add a custom format by clicking the **Create new output** button. In Create new output dialog, enter the name and check values which you want to include (these will show as columns in the result). Confirm you choice by the **Save** button. The new filter will be available in the output format combo box. The output formats can be modified or deleted using corresponding buttons next to the format name in the output combo box.

Like the chart, the table with results supports the context menu. The menu is available only at the items which can be further analyzed (ie. IP addresses). Each address can be used as a source for a next drill-down query.

Context menu can be also used for renaming important values in table, thereby you can achieve better arrangement and you won't have to remember complicated addresses. Click the address you want to rename by the right button and select **Rename** option. New names are common for all the users of the probe and do not affect function of the network.



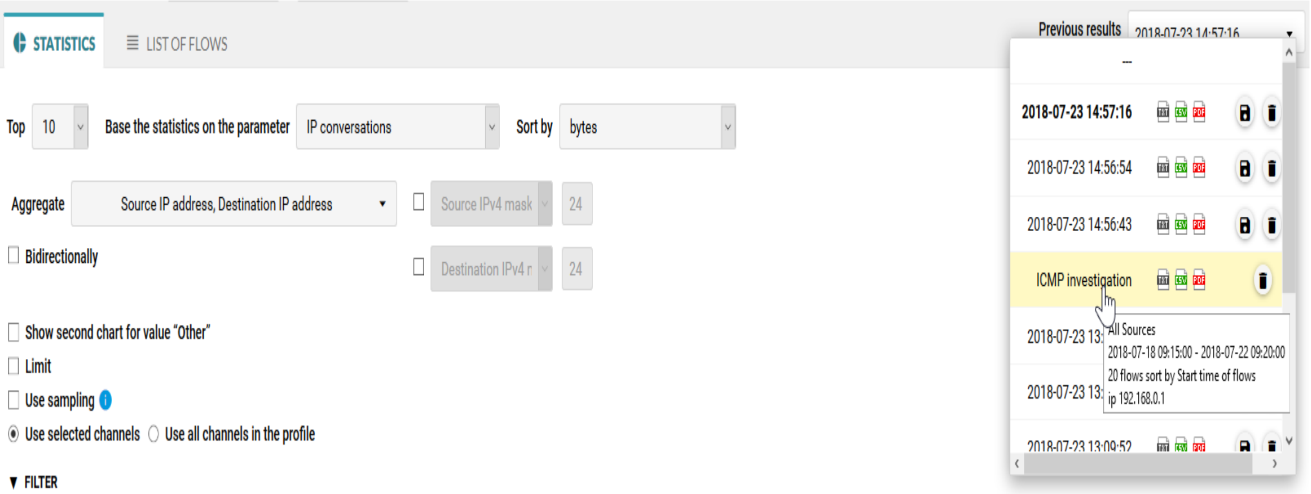
START TIME – FIRST SEEN	DURATION	PROTOCOL	SOURCE IP ADDRESS	SOURCE PORT	DESTINATION IP ADDRESS	DESTINATION PORT	TCP FLAGS	TOS	PACKETS	DEFAULT BYTES: INPUT
2018-07-19 14:19:25.084	0 s	UDP	[redacted]			ideafarm-door	....	Best Effort & Default	1	94
2018-07-19 14:19:25.174	0 s	UDP	fe80::25			ntp	....	Best Effort & Default	1	96
2018-07-19 14:19:25.450	0 s	ARP	0.0.0.0 ?			0	....	Best Effort & Default	4	112
2018-07-19 14:19:26.154	0 s	UDP	[redacted]	3335		ideafarm-door	....	Best Effort & Default	1	94
2018-07-19 14:29:04.634	0 s	UDP	gateway	492		28262	....	Best Effort & Default	1	76
2018-07-19 14:47:38.912	13.013 s	TCP	gateway			0	....	Best Effort & Default	2	152
2018-07-19 15:29:19.996	0 s	ICMP6	:: ?	N/		hbor Solicitation	....	Best Effort & Default	1	64
2018-07-19 15:29:21.008	0 s	ICMP6	fe80::250:56ff:fe9e:d00c	N/		uter Solicitation	....	Best Effort & Default	1	56

Context menu over list of flows

The Previous Results Menu

Analysis page stores the last 10 result queries for each user. These last results are available in the Previous results menu - details for each item can be displayed by hovering mouse over it. Selecting an item from this menu will set the Analysis page forms into the state corresponding to the query and display the query result. The result is just taken from database - it is not computed again, so the operation is very fast.

Each result can be exported to PDF, CSV or TXT by clicking corresponding icon. By clicking on the floppy disk icon, important results can be stored permanently with specified name. Such result will not be rewritten by new results. Each user can permanently store up to 10 result along with last 10 results. So each user is able to have up to 20 results in last results menu.



Top 10

Base the statistics on the parameter IP conversations

Sort by bytes

Aggregate Source IP address, Destination IP address

□ Source IPv4 mask 24

□ Destination IPv4 r 24

□ Bidirectionally

□ Show second chart for value "Other"

□ Limit

□ Use sampling

● Use selected channels ○ Use all channels in the profile

Previous results 2018-07-23 14:57:16

2018-07-23 14:57:16

2018-07-23 14:56:54

2018-07-23 14:56:43

ICMP investigation

2018-07-23 13:

2018-07-23 13:

2018-07-23 13:09:52

All Sources
2018-07-18 09:15:00 - 2018-07-22 09:20:00
20 flows sort by Start time of flows
ip 192.168.0.1

Previous results

Reports

Flowmon device supports automatic generation of network traffic statistics. The outputs can be pie charts, flow charts or tables. Usage of this function does not require deeper knowledge of network problematics. Nevertheless, it provides all information necessary for access supervision of both Internet and local network servers. It allows to check structure of traffic and used services, to find stations most loading the crucial network connections, to plan capacity network connections properly and a lot of more.

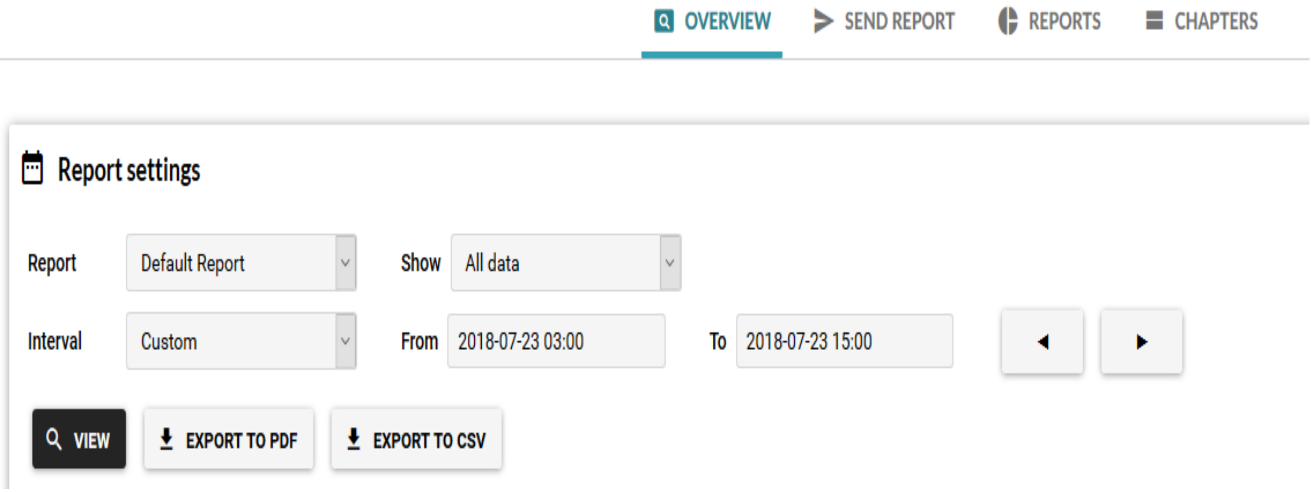
Measured data is viewed in form of reports, which are user-defined listings of tables and charts. Report statistics are stored with 1-hour granularity. The basic element of reports are chapters, which contain particular measurements. Chapter is defined by its name, description, type of statistic and filter. Chapters are represented as separate pages in the report and they contain parameters of measurement and resulting table, chart or both. Creation of statistics for particular chapters is computationally demanding task and therefore the chapters can be created only by the system administrator. The rest of users can create their own reports using predefined chapters only. Detailed settings of reports and chapters will be described later in this chapter.

The Reports page contains the following four tabs:

- **Overview** - views reports.
- **Send report** - configuration of sending reports to email or external storage.
- **Reports** - used for report management.
- **Chapters** - creating and managing chapters which can be used in reports.

Overview Tab

Overview tab is a place where users can display their own reports. There is form on the top of the page which allows to select report and additional options. Select the requested time interval from the **Interval** combo box (or set your own using text boxes From and To) and press the **View** button to display a report. If you want to show working hours in the flow charts, select their definition from the Show combo box. Generated report can be also exported to PDF or CSV file using **Export to PDF** and **Export to CSV** buttons.



Report: Default Report
Show: All data
Interval: Custom
From: 2018-07-23 03:00
To: 2018-07-23 15:00

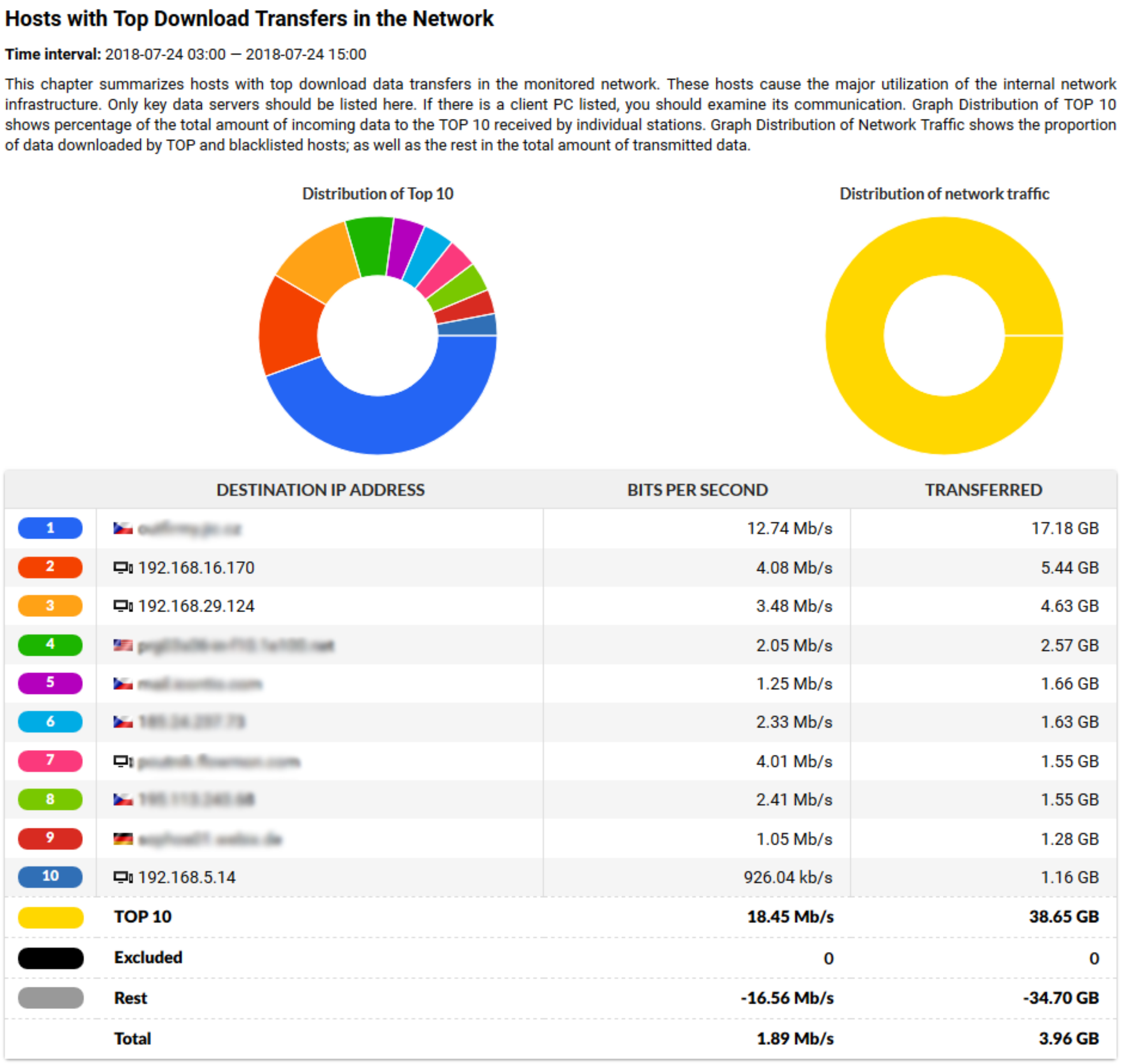
Show report panel

As it was already said, the report consists of one or more chapters which are represented as separated "sheets of paper" and are in the same way exported to PDF file. You can switch between particular chapters using links in the "Content" floating window (it can be minimized by clicking its title bar). The chapter starts by its name, then there is processed time range, selected working hours and detailed description. There are two types of chapters - Top and Traffic.

Top chapters

Top chapters display the top items (hosts, ports etc.) in the network traffic according to the specified criterion (eg. number of transmitted bytes, packets etc.).

There are pie charts of top 10 most important hosts. Under the charts there are tables containing detailed statistics (including aggregated data).



Hosts with Top Download Transfers in the Network

Time interval: 2018-07-24 03:00 — 2018-07-24 15:00

This chapter summarizes hosts with top download data transfers in the monitored network. These hosts cause the major utilization of the internal network infrastructure. Only key data servers should be listed here. If there is a client PC listed, you should examine its communication. Graph Distribution of TOP 10 shows percentage of the total amount of incoming data to the TOP 10 received by individual stations. Graph Distribution of Network Traffic shows the proportion of data downloaded by TOP and blacklisted hosts; as well as the rest in the total amount of transmitted data.

	DESTINATION IP ADDRESS	BITS PER SECOND	TRANSFERRED
1	[redacted]	12.74 Mb/s	17.18 GB
2	192.168.16.170	4.08 Mb/s	5.44 GB
3	192.168.29.124	3.48 Mb/s	4.63 GB
4	[redacted]	2.05 Mb/s	2.57 GB
5	[redacted]	1.25 Mb/s	1.66 GB
6	[redacted]	2.33 Mb/s	1.63 GB
7	[redacted]	4.01 Mb/s	1.55 GB
8	[redacted]	2.41 Mb/s	1.55 GB
9	[redacted]	1.05 Mb/s	1.28 GB
10	192.168.5.14	926.04 kb/s	1.16 GB
🟨	**TOP 10**	**18.45 Mb/s**	**38.65 GB**
⬛	**Excluded**	**0**	**0**
▨	**Rest**	**-16.56 Mb/s**	**-34.70 GB**
	Total	**1.89 Mb/s**	**3.96 GB**

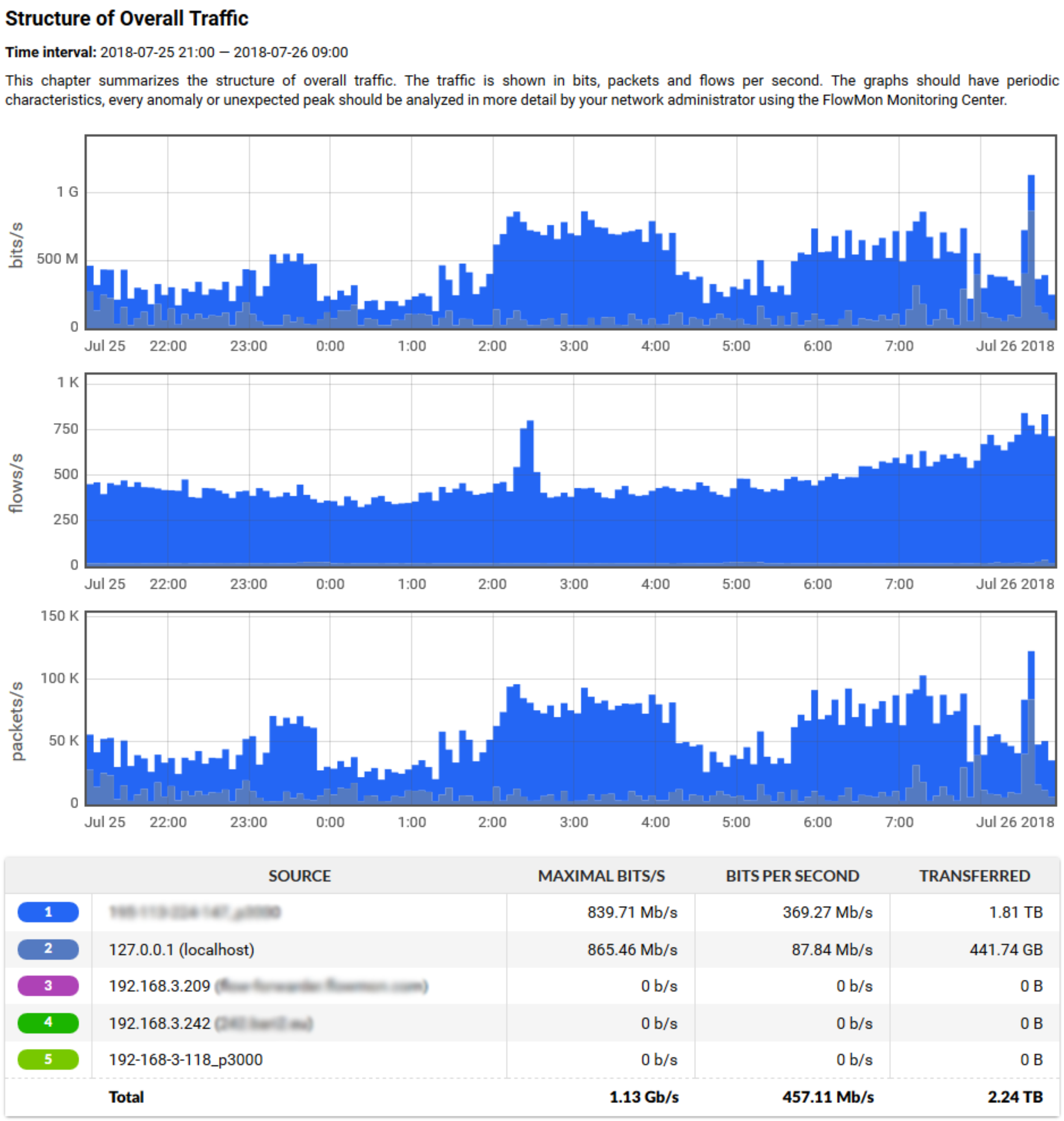
Top chapter

Traffic chapters

Traffic chapters display history of network traffic during selected time interval.

The chapter shows three charts displaying number of flows, transferred packets and bits (volumetric data). When a chart is hovered by the mouse, a floating menu appears. It allows to switch between the linear and logarithmic axis y and between the line and stacked chart. Below there is a table containing detailed statistics. It is necessary the have Traffic charts enabled in channel options, otherwise, no Volumetric data will be shown.

If Performance data are selected for the Traffic chapter, there is an extra chart for NPM metrics data below the statistics table. It is necessary the have NPM charts enabled in channel options, otherwise, no Performance data will be shown.



Structure of Overall Traffic

Time interval: 2018-07-25 21:00 — 2018-07-26 09:00

This chapter summarizes the structure of overall traffic. The traffic is shown in bits, packets and flows per second. The graphs should have periodic characteristics, every anomaly or unexpected peak should be analyzed in more detail by your network administrator using the FlowMon Monitoring Center.

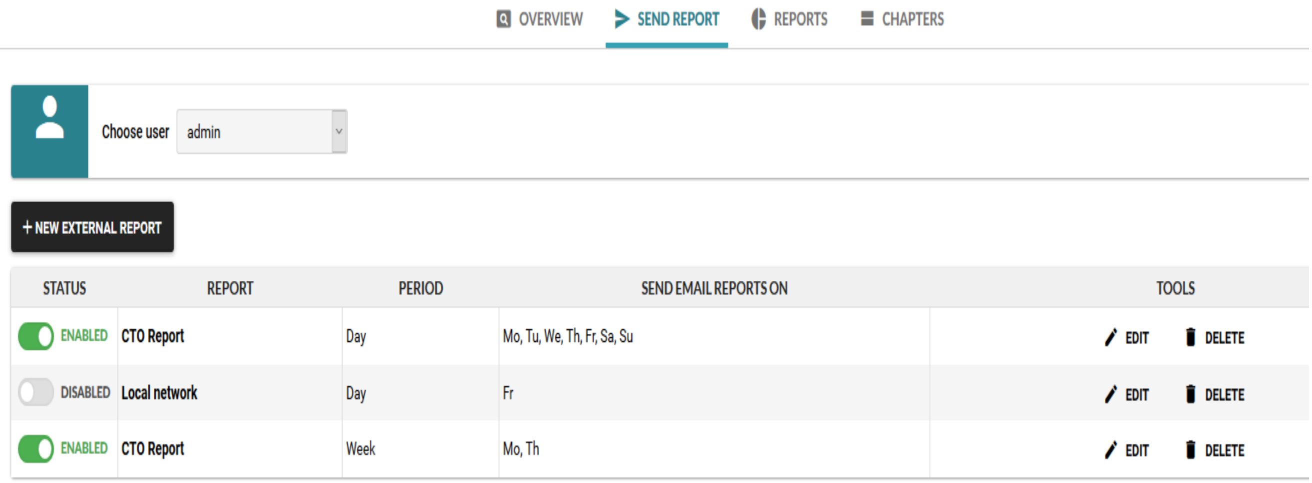
	SOURCE	MAXIMAL BITS/S	BITS PER SECOND	TRANSFERRED
1	[redacted]	839.71 Mb/s	369.27 Mb/s	1.81 TB
2	127.0.0.1 (localhost)	865.46 Mb/s	87.84 Mb/s	441.74 GB
3	192.168.3.209 [redacted]	0 b/s	0 b/s	0 B
4	192.168.3.242 [redacted]	0 b/s	0 b/s	0 B
5	192-168-3-118_p3000	0 b/s	0 b/s	0 B
	Total	**1.13 Gb/s**	**457.11 Mb/s**	**2.24 TB**

Traffic chapter

Send Report Tab

Flowmon allows to automatically generate reports and send them to email or remote storage. The Send report tab is used to configure this feature. To enable sending reports to remote storage, you need to configure external storage connection in Configuration center (please see chapter External Data Storage). Furthermore, it is necessary to configure parameters of remote reports sending process. This can be done in Configuration Center in Flowmon Monitoring Center configuration page (see chapter Reports settings).

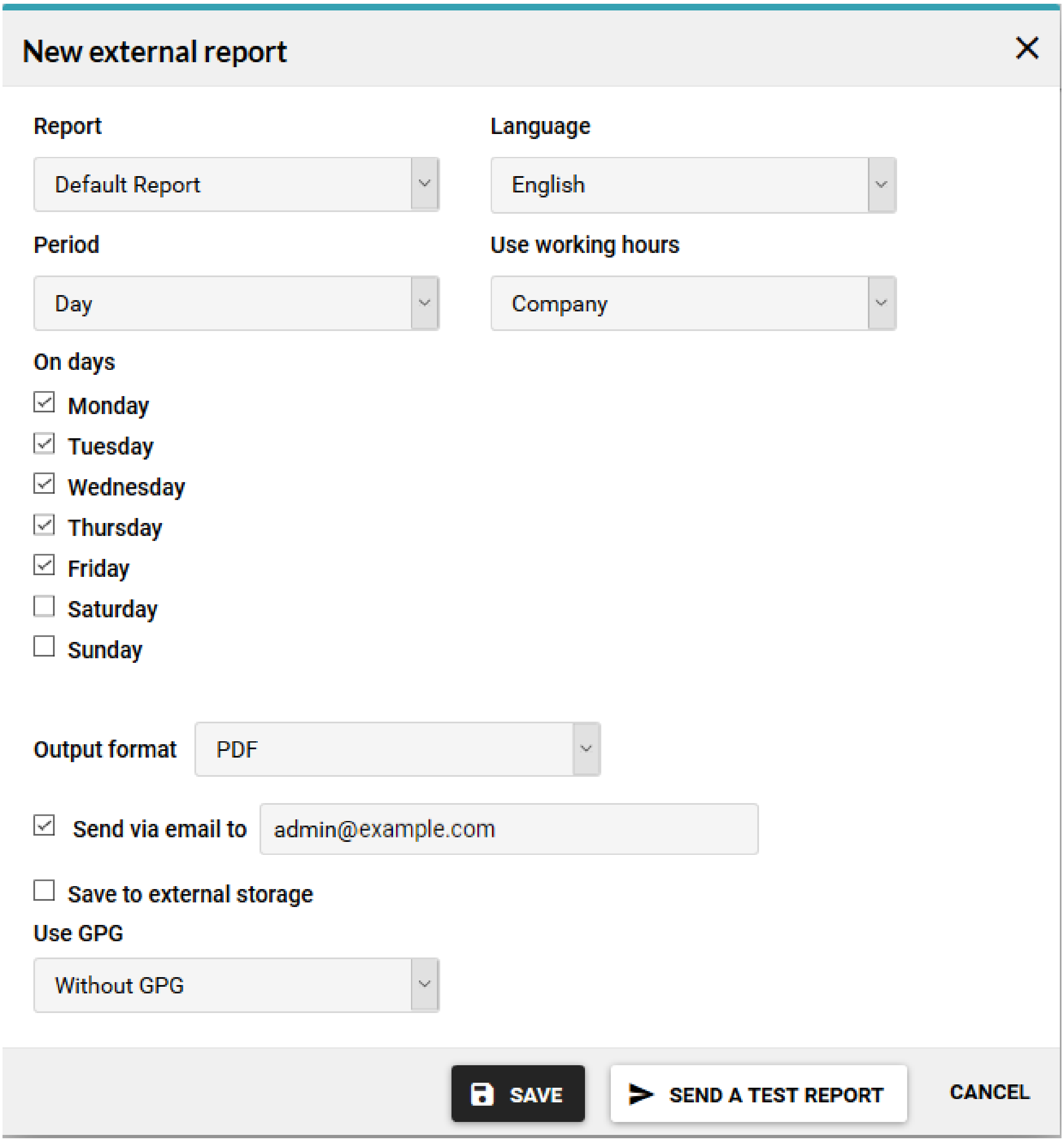
There is **Choose user** combo box on the top of the form. This box is shown only to the system administrator, other users can configure only their own reports. Below there is list of reports and intervals of their generation. The report is created and sent only if its status is set to enabled. Reports can be managed by buttons in the Tools column. A new report can be created by clicking on the **New external report** button.



STATUS	REPORT	PERIOD	SEND EMAIL REPORTS ON	TOOLS
ENABLED	CTO Report	Day	Mo, Tu, We, Th, Fr, Sa, Su	EDIT DELETE
DISABLED	Local network	Day	Fr	EDIT DELETE
ENABLED	CTO Report	Week	Mo, Th	EDIT DELETE

List of reports to send

By clicking on this button New external form is shown. Choose report for configuration. Then set a language, time period, requested working hours and output format. Then choose whether to send report via email (use comma-separated list of email addresses) or save it to an external storage. There is also an option to use GPG. Create report by clicking the **Save** button.



New external report

Report: Default Report

Language: English

Period: Day

Use working hours: Company

On days

☑ Monday

☑ Tuesday

☑ Wednesday

☑ Thursday

☑ Friday

□ Saturday

□ Sunday

Output format: PDF

☑ Send via email to: admin@example.com

□ Save to external storage

Use GPG: Without GPG

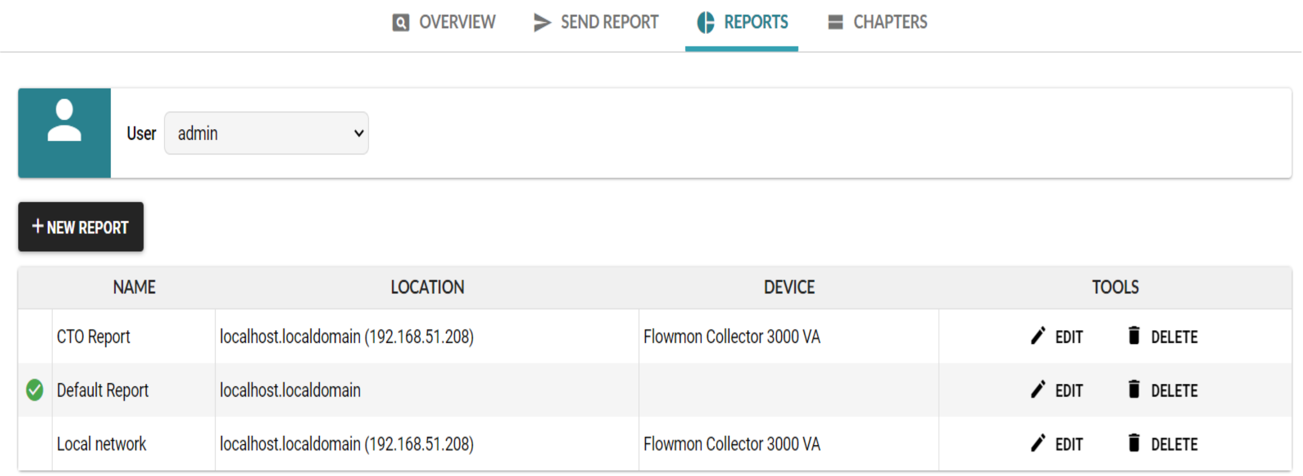
Report to send settings panel

Reports of all users are sent every day at 1:25 am. First a list of reports to generate is created, then the reports are generated and sent. The only exception is made up by reports with user-defined time interval. Such reports are generated approximately in 15th minute of the defined hour.

Reports Tab

The Reports tab allows to add, modify and delete reports. You can view defined reports on the Overview tab or set them to be sent by email on the Email reports tab.

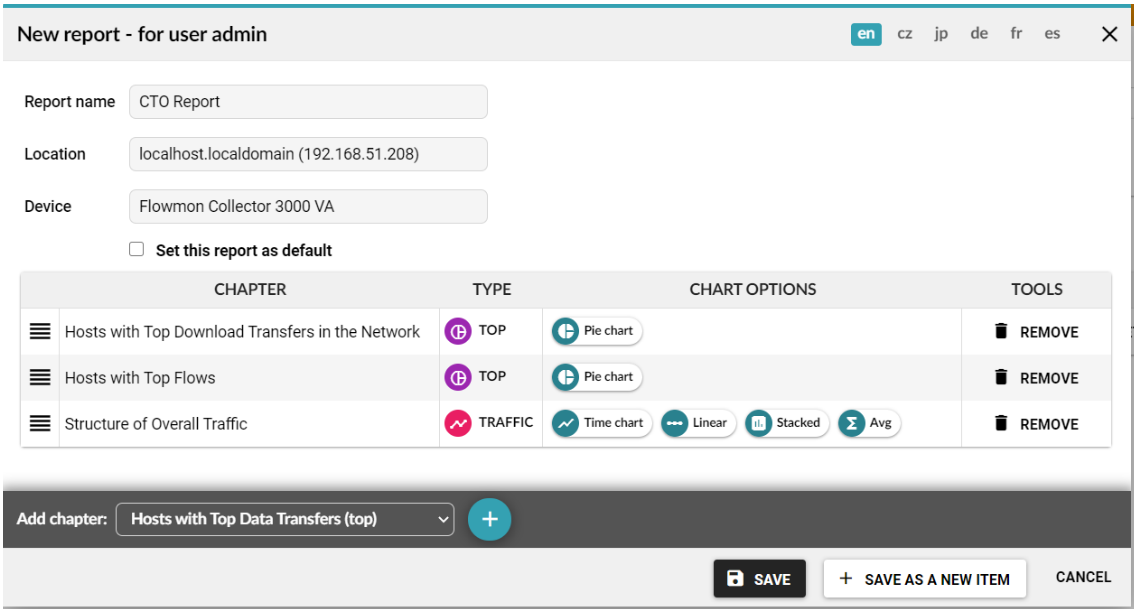
Existing reports can be maintained using buttons in the Tools column, new report can be created by clicking the **New report** button. The system administrator can create and modify reports of any user whose name was selected in the combo box above the table. The **New report** button opens the Edit report dialog box.



User admin

NAME	LOCATION	DEVICE	TOOLS
CTO Report	localhost.localdomain (192.168.51.208)	Flowmon Collector 3000 VA	EDIT DELETE
✓ Default Report	localhost.localdomain		EDIT DELETE
Local network	localhost.localdomain (192.168.51.208)	Flowmon Collector 3000 VA	EDIT DELETE

Report list



New report - for user admin

Report name: CTO Report

Location: localhost.localdomain (192.168.51.208)

Device: Flowmon Collector 3000 VA

□ Set this report as default

CHAPTER	TYPE	CHART OPTIONS	TOOLS
Hosts with Top Download Transfers in the Network	TOP	Pie chart	REMOVE
Hosts with Top Flows	TOP	Pie chart	REMOVE
Structure of Overall Traffic	TRAFFIC	Time chart, Linear, Stacked, Avg	REMOVE

Add chapter: Hosts with Top Data Transfers (top)

Report configuration

The dialog box is divided into two parts - the upper part contains descriptive information while the bottom part allows to choose the chapters to include to the report.

Flowmon allows to create reports in various languages. To make this function work correctly it is necessary to fill in the report name and the rest of descriptive information for each language separately. The language can be changed in its upper right corner next to the close button. Before saving of the report you should fill in its description in all languages that you are going to use.

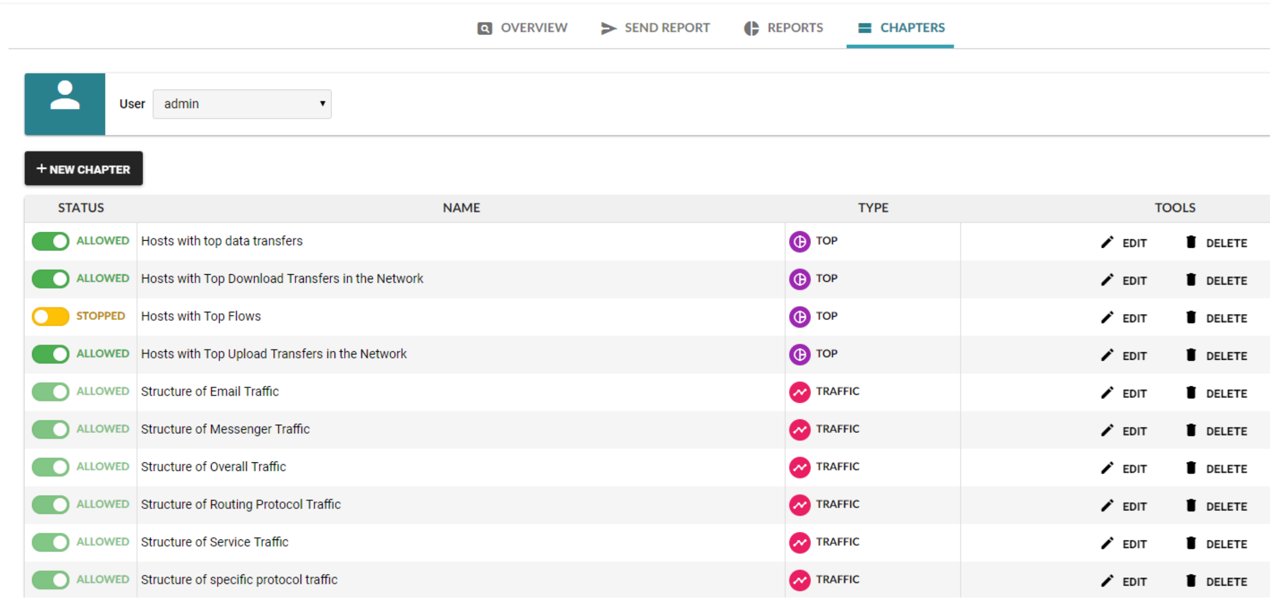
The table at the bottom displays a list of chapters included in the report. If you want to add a new chapter, choose its name from the combo box below the table and press the **Add new chapter** button. This inserts the chapter at the end of the list. If you want to put it on some other place, drag it by the left mouse button. If the combo box of available chapters does not contain the chapter you want to add, probably you don't have permissions to use it. In such case contact the system administrator and ask them for granting privileges for that chapter.

Buttons in the Tools column are used to work with particular chapters. Use the **Remove** button to exclude the chapter from the report (the chapter itself is not deleted). At the traffic chapters two additional buttons are displayed. These buttons allow to change the default appearance of the flow charts. The green chart icon turns on the stacked chart while the bar chart toggles linear and logarithmic scale of the axis y.

Create new report by clicking the **Save** button.

Chapters Tab

The Chapters tab allows to manage chapters which can be included to reports. The calculation of data for particular chapters is a computationally demanding task and therefore the chapters can be managed only by users with full access to FMC, while the other users may choose from the prearranged chapters only.



User admin

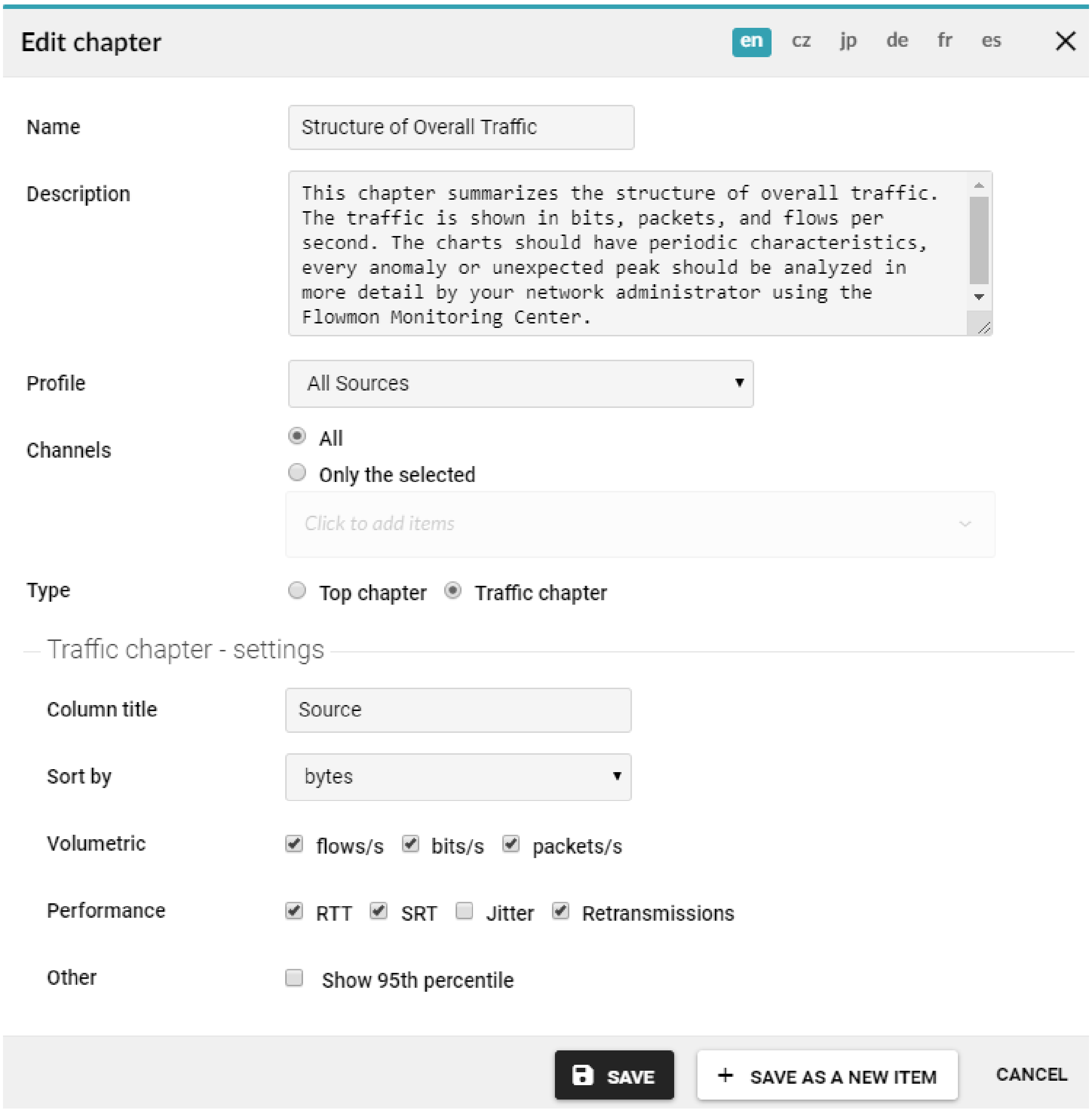
STATUS	NAME	TYPE	TOOLS
ALLOWED	Hosts with top data transfers	TOP	EDIT DELETE
ALLOWED	Hosts with Top Download Transfers in the Network	TOP	EDIT DELETE
STOPPED	Hosts with Top Flows	TOP	EDIT DELETE
ALLOWED	Hosts with Top Upload Transfers in the Network	TOP	EDIT DELETE
ALLOWED	Structure of Email Traffic	TRAFFIC	EDIT DELETE
ALLOWED	Structure of Messenger Traffic	TRAFFIC	EDIT DELETE
ALLOWED	Structure of Overall Traffic	TRAFFIC	EDIT DELETE
ALLOWED	Structure of Routing Protocol Traffic	TRAFFIC	EDIT DELETE
ALLOWED	Structure of Service Traffic	TRAFFIC	EDIT DELETE
ALLOWED	Structure of specific protocol traffic	TRAFFIC	EDIT DELETE

Chapters list

The table shows all the chapters defined in the system. The status column displays whether the user selected in the combo box above the table has permission to use the chapter. It depends on whether the user has access to the profile over which the chapter is defined. To edit chapters, you can use tools in the tools column. Use the **New chapter** button to add a new chapter.

Enter name and detailed description for the new chapter. If you are going to generate reports in various languages, do not forget to fill in the information for all languages you want to use. You can switch between them using the buttons in the top right corner next to the close button.

Choose input data for chapter in the profile box. If you are creating a traffic chapter, you can use also shadow profiles. For further information about differences between the top and traffic chapters see the Overview Tab chapter.



Name: Structure of Overall Traffic

Description: This chapter summarizes the structure of overall traffic. The traffic is shown in bits, packets, and flows per second. The charts should have periodic characteristics, every anomaly or unexpected peak should be analyzed in more detail by your network administrator using the Flowmon Monitoring Center.

Profile: All Sources

Channels: ● All ○ Only the selected

Click to add items

Type: ○ Top chapter ● Traffic chapter

Traffic chapter - settings

Column title: Source

Sort by: bytes

Volumetric: ☑ flows/s ☑ bits/s ☑ packets/s

Performance: ☑ RTT ☑ SRT ☐ Jitter ☑ Retransmissions

Other: ☐ Show 95th percentile

Edit chapter

Warning

Deleting chapter in a sub-tenant leads to a removal of the chapter from every location in the system! Chapters are not tenant-based entities.

Common Options

- **Name** - name of the chapter
- **Description** - additional description of the chapter
- **Profile** - profile used as a source of data for the chapter
- **Channels** - channels used as a source of data for the chapter
  - Select **All** for all channels including those added in the future
  - Select **Only the selected** for selecting the specific channels only
- **Type** - Select **Top chapter** or **Traffic chapter**

Top Chapter Options

- **Top** - number of rows of the statistics
- **Base the statistics on the parameter** - select the key for the statistics
- **Sort by** - column to sort the statistics by
- **Chapter columns** - columns to be displayed in the table. The value in the last column always corresponds to the value selected in the **Sort by** combo box
- **Filter** - allows to enter a filter for the processed traffic

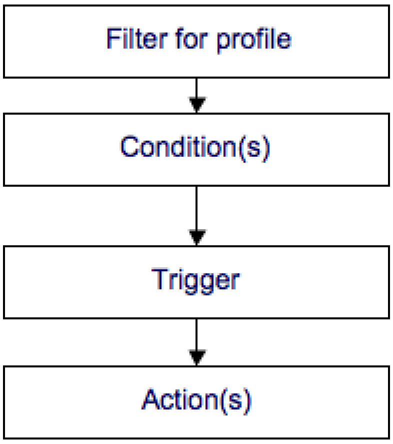
Traffic Chapter Options

- **Column title** - description of the first table column
- **Sort by** - column to sort the table by
- **Volumetric** - select the list of volumetric data to display in chart
- **Performance** - select the list of performance data to display in chart
- **Show 95th percentile** - turns on showing of 95% percentile in the tables (for both transfer rate and transferred data)

Alerts

Flowmon Monitoring Center allows to automatically watch predefined network abnormalities and trigger specified action when they appear. These watches are called alerts and they are defined using filters of the selected profile, conditions of execution, type of trigger and action to be performed. Alerts are available for the 5m, 1m and 30s profiles. The 1m and 30s profiles' alerts are evaluated every 30s, and similarilly, the 5m profiles' alerts are evaluated every 5 minutes.

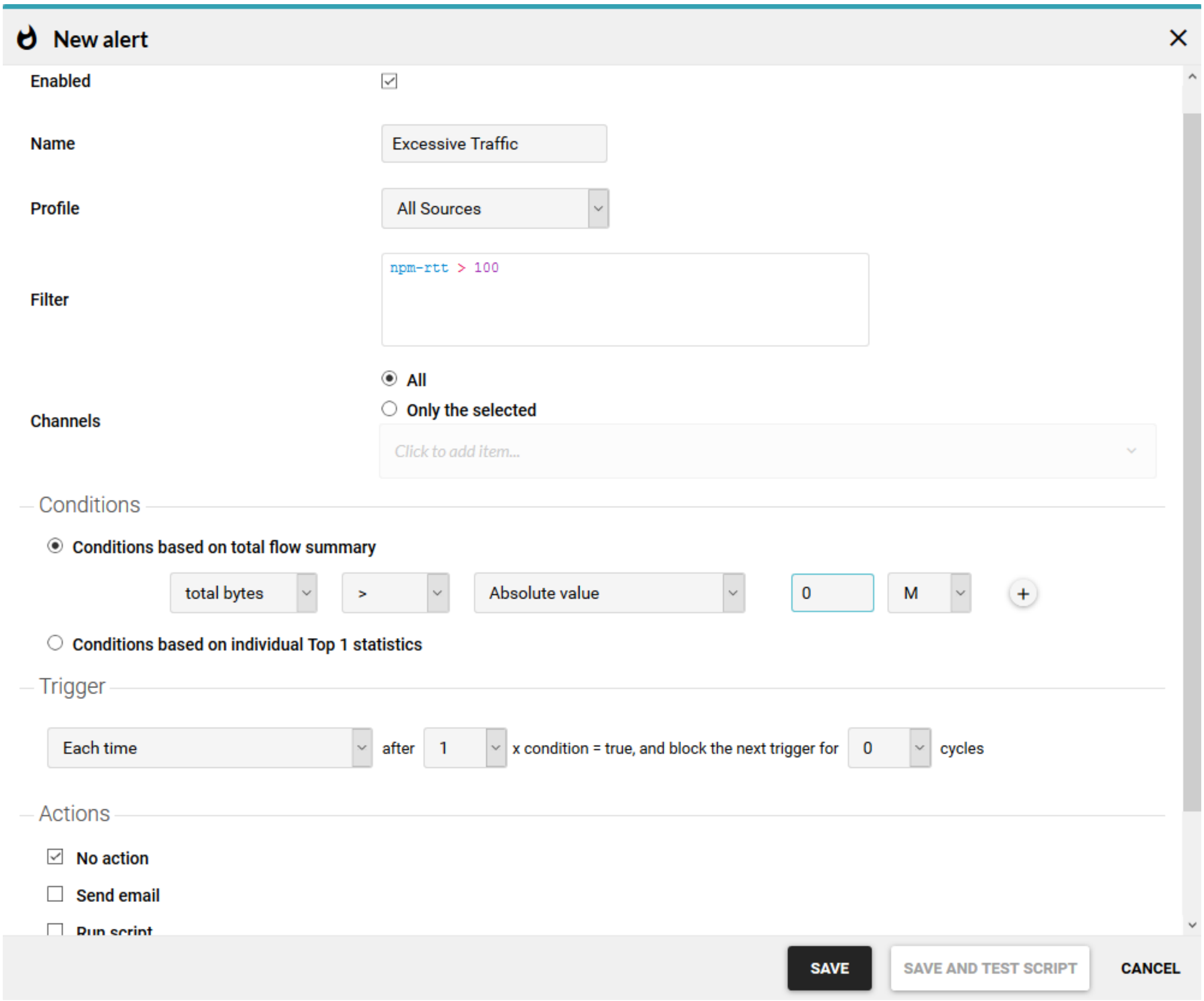
The list of all alerts and theirs statuses is displayed on the Alerts page. Details about the particular alerts can be displayed by clicking the **Details** button.



Alert activation process

Creating New Alert

New alert can be created by clicking the **New alert** button and filling the New alert form.



Enabled	☑
Name	Excessive Traffic
Profile	All Sources
Filter	`npm-rtt > 100`
Channels	● All ○ Only the selected Click to add item...

Conditions

● Conditions based on total flow summary

total bytes | > | Absolute value | 0 | M | +

○ Conditions based on individual Top 1 statistics

Trigger

Each time after 1 x condition = true, and block the next trigger for 0 cycles

Actions

☑ No action

□ Send email

□ Run script

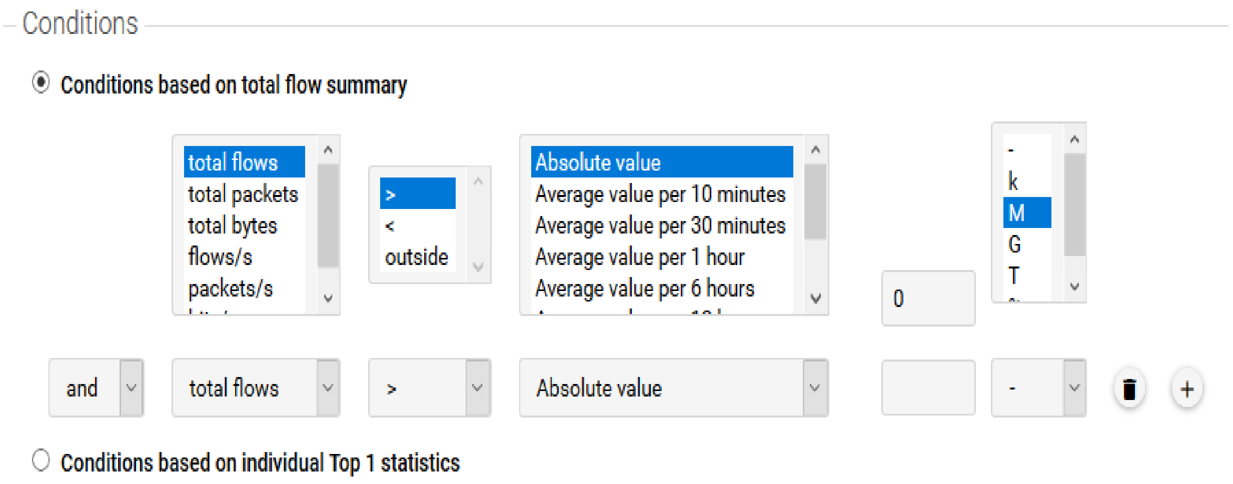
New alert form

- **Profile** - Select parent profile.
- **Channels** - Select channels with data relevant to alert. Option "All" means all channels including those added in the future.
- **Filter** - Enter filter of alert related to the parent profile. Conditions of execution depend on this filter.
- **Conditions of execution** - Conditions of execution are defined either over a list of flows (Conditions based on total flow summary) or over a flow statistics (Conditions based on individual Top 1 statistics) and they can be connected together (up to 6 conditions). New condition can be added by clicking the plus icon on the right side of the condition parameters. At the beginning of the second and all the following conditions it is possible to choose a connective used to connect the condition with the previous one (and / or).

  Conditions of execution can be defined, for example, for the number of flows, packets, bytes or NPM metrics going trough the filter. This number is compared either with absolute value, with average value for selected time interval or with weekly baseline. This allows to define adaptive filters for easy detection of peaks.

  The **weekly baseline** is applied only, if profile history is at least 7 days long. Traffic amount for current 5 minutes is compared with average value for the same 5 minutes in the same day of weeks (e.g. value for Monday 12:10 is compared to previous Mondays 12:10). The longer the profile history is, the better results this method provides. The maximum length of the history is 28 days (i.e. four weeks).

  Also, it is possible to define the conditions of execution over Top 1 statistics.

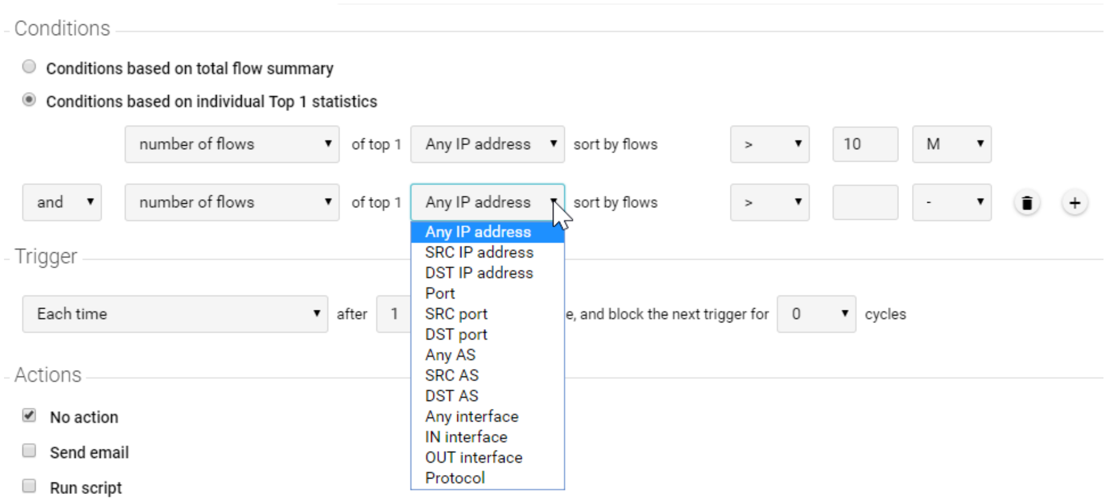


Conditions

● Conditions based on total flow summary

○ Conditions based on individual Top 1 statistics

Alert condition settings



Conditions

○ Conditions based on total flow summary

● Conditions based on individual Top 1 statistics

Trigger

Each time after 1 … e, and block the next trigger for 0 cycles

Actions

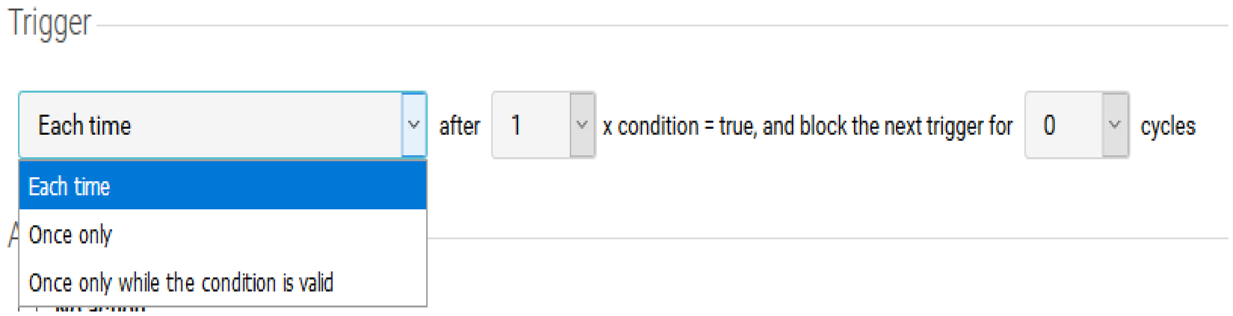
☑ No action

☐ Send email

☐ Run script

Alert condition settings

- **Trigger** - Whenever the conditions of execution are satisfied, selected action is triggered. According to your needs it is possible to set the action to trigger **Each time** the conditions are satisfied, **Once only** or **Once only while the condition is valid**. Furthermore it is possible to set that repeated satisfaction of the conditions is needed to trigger the action and when the action is triggered, you can also disable its execution for several cycles. If the trigger is set to **Once only**, the condition is invalidated after each trigger and you must activate it again by pressing the **Rearm** button in the alerts list.



Trigger

Each time after 1 x condition = true, and block the next trigger for 0 cycles

Alert activation frequency settings

- **Action** - Defines an action to be performed when the alert triggers. Usually it is sending of an email, executing user defined script (via Call plugin: runscriptplugin), sending a syslog message in CEF format (via Call plugin: syslogplugin) or sending SNMP trap (via Call plugin: snmptrapplugin). It is possible to choose more than one action. If you select **No action**, the rest of actions is unchecked and the alert is inactivated.

- When defining an **email** action, the **Recipient** field can contain one or more email addresses. Email addresses have to be separated by comma or semicolon characters.

Alerts Based on Shadow Profiles

There are some limitations when creating alerts based on a shadow profile. The limiting factor is a granularity of a parent profile used for the shadow profile definition. See the following table to find out when it is possible to create an alert based on a shadow profile.

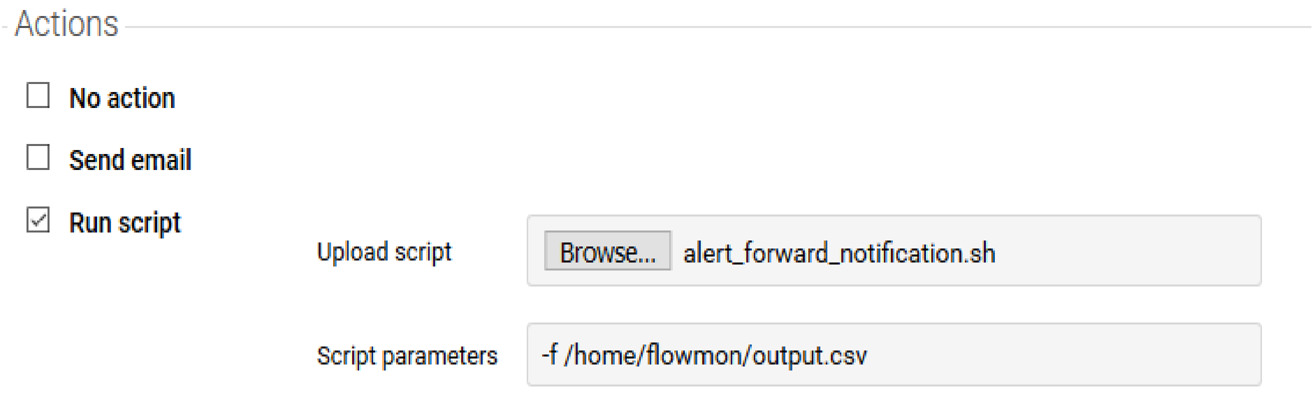
	Shadow's profile parent granularity		
	30s	1m	5m
Alert on a 30s shadow profile	✓	✓	✗
Alert on a 1m shadow profile	✓	✓	✗
Alert on a 5m shadow profile	✓	✓	✓

User-defined Scripts

As an action for alert, a user-defined BASH script can be run (when **Run script** box is checked). The script can be uploaded by pressing the button **Browse.** Script parameters can be specified in

Script parameters field.

If the alert data (name, time, conditions, measured values) are needed in the user script, it is necessary to include mandatory code (see the following example script) which sets all alert variables.



Actions

☐ No action

☐ Send email

☑ Run script

Upload script: Browse... alert_forward_notification.sh

Script parameters: -f /home/flowmon/output.csv

Run script settings

The following user script example saves alert name, timeslot and total number of bytes/packets/flows to the file defined by input parameter **f**.

Example of a user-defined script

```
# start of mandatory part of source code
. /usr/local/bin/fmc_alert_functions
if [ -L $0 ] ; then
```

```
DIR=$(dirname $(readlink -f $0)) ;
else
DIR=$(dirname $0) ;
fi ;
input_json=$(cat "$DIR/pluginscript_input")
parse_alert_data "$input_json"
# end of mandatory part of source code
# Initialize our own variables
parameter_filename=""
# Processs input parameters
while getopts "f:" opt; do
case "$opt" in
h|\?)
echo "invalid␣option␣$opt"
exit 1
;;
f) parameter_filename=$OPTARG
;;
esac
done
shift $((OPTIND-1))
[ "$1" = "--" ] && shift
echo "======ALERT␣INFO======" > $parameter_filename
echo "Alert␣name:␣$ALERT_NAME" >> $parameter_filename
echo "Alert␣timeslot:␣$ALERT_TIMESLOT" >> $parameter_filename
echo "======ALERT␣DATA======" >> $parameter_filename
echo "Summary␣bytes:␣$SUMMARY_BYTES" >> $parameter_filename
echo "Summary␣packets:␣$SUMMARY_PACKETS" >> $parameter_filename
echo "Summary␣flows:␣$SUMMARY_FLOWS" >> $parameter_filename
```

List of variables

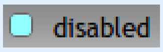
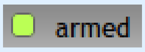
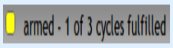
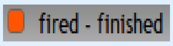
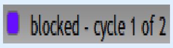
```
ALERT_BASED_ON=Alert based on "summary" or "TOP1" statistic
ALERT_NAME=Alert's displayed name
ALERT_TIMESLOT=Timeslot
INTERNAL_NAME=Alert's identifier (UUID)
#Summary data
SUMMARY_BYTES=Number of bytes
SUMMARY_PACKETS=Number of packets
SUMMARY_FLOWS=Number of flows
SUMMARY_BPS=Bits per second
SUMMARY_PPS=Packet per second
SUMMARY_BPP=Bits per packet
#Top1 data
TOP1_DATA=Top1 data
#Conditions and its values
CONDITION_COUNTER=Number of conditions
CONDITION1_WHAT=Condition by
flows/packets/bytes/flows_per_second/packets_per_second/bits_per_second
CONDITION2_WHAT
CONDITION3_WHAT
CONDITION4_WHAT
CONDITION5_WHAT
CONDITION6_WHAT
CONDITION1_COMPARE_BY=Comparision operator and value to compare
CONDITION2_COMPARE_BY
CONDITION3_COMPARE_BY
CONDITION4_COMPARE_BY
CONDITION5_COMPARE_BY
CONDITION6_COMPARE_BY
CONDITION1_ACTUAL_VALUE=Current measured value
CONDITION2_ACTUAL_VALUE
CONDITION3_ACTUAL_VALUE
CONDITION4_ACTUAL_VALUE
CONDITION5_ACTUAL_VALUE
CONDITION6_ACTUAL_VALUE
CONDITION1_AVERAGE_VALUE=Average value for X minutes/hours/days (only for average values)
```

```
CONDITION2_AVERAGE_VALUE
CONDITION3_AVERAGE_VALUE
CONDITION4_AVERAGE_VALUE
CONDITION5_AVERAGE_VALUE
CONDITION6_AVERAGE_VALUE
CONDITION1_RESULT=How the condition was evaluated "True" or "False"
CONDITION2_RESULT
CONDITION3_RESULT
CONDITION4_RESULT
CONDITION5_RESULT
CONDITION6_RESULT
CONDITION1_BINARY_OPERATION=Binary operation of condition "OR" or "AND"
CONDITION2_BINARY_OPERATION
CONDITION3_BINARY_OPERATION
CONDITION4_BINARY_OPERATION
CONDITION5_BINARY_OPERATION
CONDITION6_BINARY_OPERATION
```

To test the correct function of the script, click on the **Save and test script** button. A window will pop up with information about each performed script action.

Alert Status

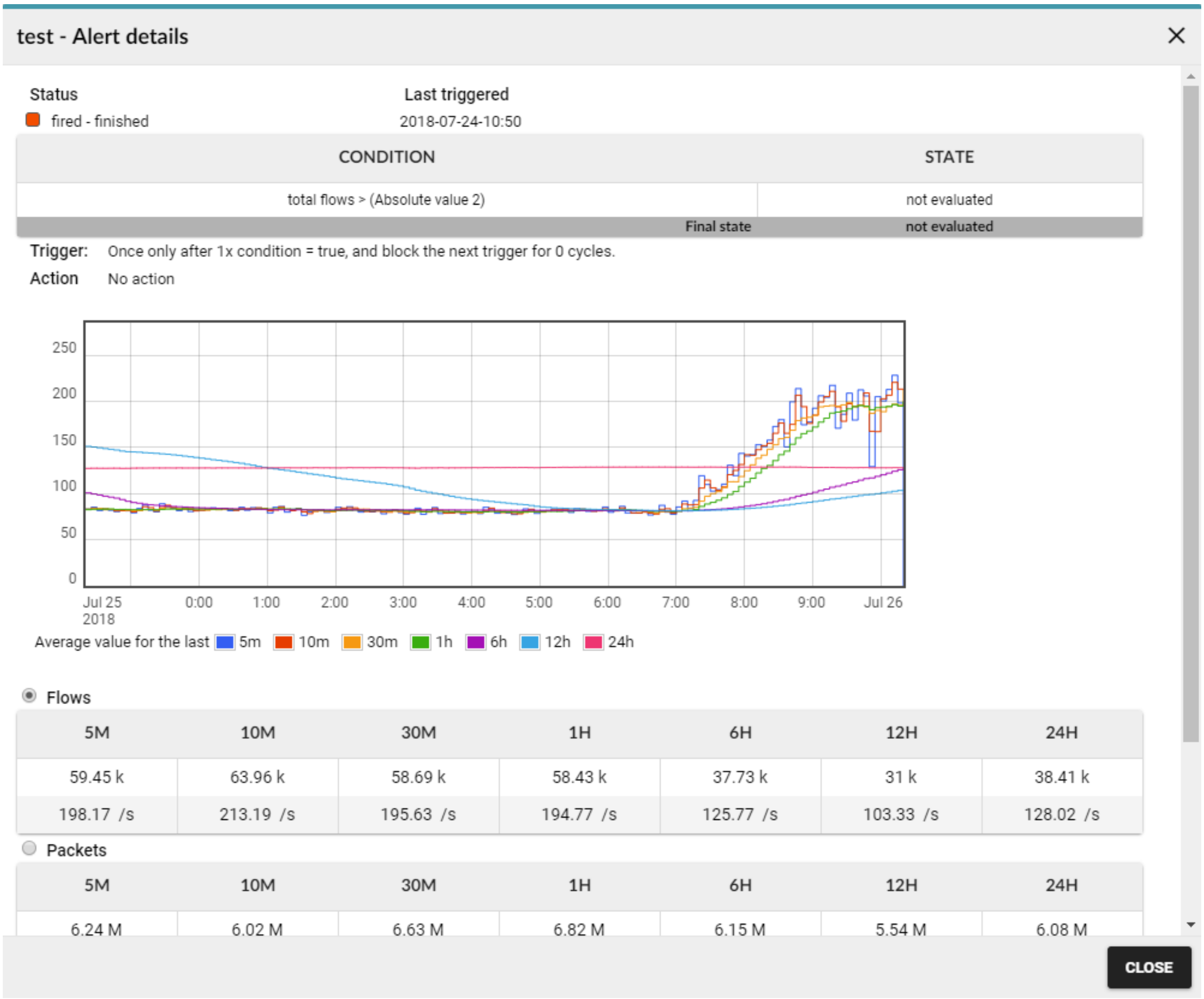
The alert status is displayed in the Status column of the alerts table and it is also visible in the top left corner of alert details dialog. The status can be one of the following:

Status	Description
 disabled	This alert is not active and it is not evaluated.
 armed	This alert is active and its conditions are evaluated each cycle.
 armed - 1 of 3 cycles fulfilled	This alert is active and is evaluated each cycle. The last overall condition was true, but needs 3 conditions (definable) in a row to fire the trigger. So far, the condition was satisfied only once.
fired	This alert is active and it is evaluated each cycle. The trigger just fired in the last cycle and executed the action assigned to this alert.
 fired - finished	This alert fired once only and it is no longer active. The alert needs to be rearmed manually.
 blocked - cycle 1 of 2	This alert is active, but blocked for 2 cycles (definable) after the trigger fired. Currently one of the two blocked cycles are already over.

Alert Details

After clicking the **Details** button in the alerts list, the following form shows up. It displays details of selected alert.

In the upper part of the form there is current status of alert, date and time of its last trigger, state of conditions evaluation and action to be performed. The bottom part of the form contains chart showing flow of average network traffic values. Values in the chart can be used to make more exact specification of conditions of execution. The vertical cursor (vertical lines) in the chart marks when the trigger was lastly triggered. The 30s alert chart has a 30s granularity, the 5m alert chart a 5m granularity.



test - Alert details

Status
🟥 fired - finished

Last triggered
2018-07-24-10:50

CONDITION		STATE
total flows > (Absolute value 2)		not evaluated
	Final state	not evaluated

Trigger: Once only after 1x condition = true, and block the next trigger for 0 cycles.

Action No action

● Flows

5M	10M	30M	1H	6H	12H	24H
59.45 k	63.96 k	58.69 k	58.43 k	37.73 k	31 k	38.41 k
198.17 /s	213.19 /s	195.63 /s	194.77 /s	125.77 /s	103.33 /s	128.02 /s

○ Packets

5M	10M	30M	1H	6H	12H	24H
6.24 M	6.02 M	6.63 M	6.82 M	6.15 M	5.54 M	6.08 M

Alert details form

The table under the chart displays average values of the network traffic measured during the last time slot in flows, packets and bytes. The radio buttons above the tables can be used to switch the chart units.

For instance, the 30m average value is calculated from last 6 timeslots. Each timeslot covers 5 minutes, so 6 * 5m = 30m. Sum of flows within these timeslots is divided by 6 and the result is presented as 30 minute average. This value is than compared with current 5-minute timeslot according to alert rule.

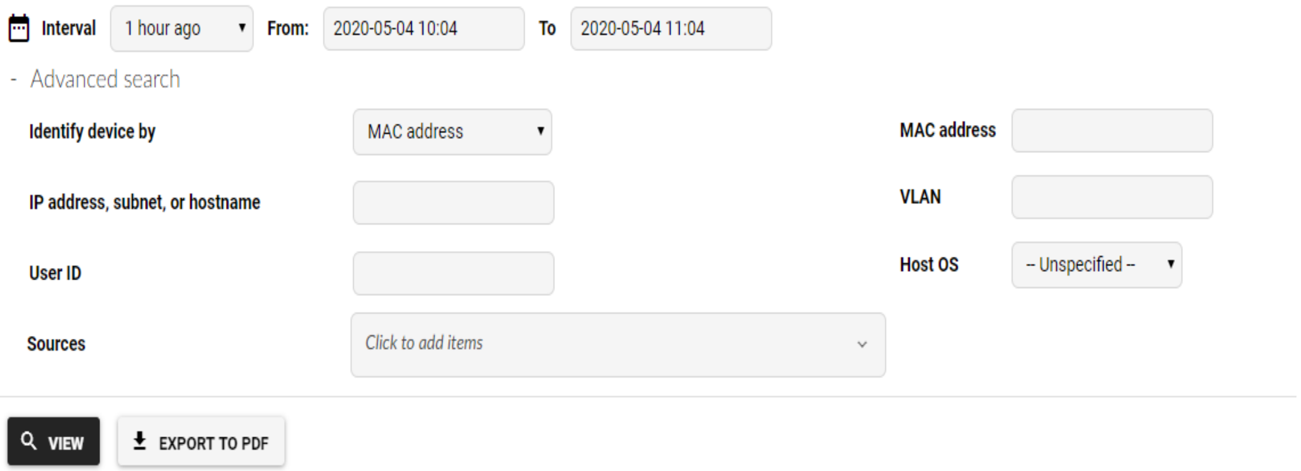
Active Devices

Flowmon Monitoring Center allows you to display list of devices that communicate on the network at some point in time. By default, this service is turned off and you need to turn it on in the Flowmon Configuration Center - FMC Configuration in Active Devices - Basic settings.

On the page Active Devices, you can see a search form, Overview tab and List tab. Overview tab displays tables with interesting information about monitored network, such as Top vendors, Active devices in time etc. List tab contains a table listing devices that communicated on the network in the defined interval. If there are more than 100 entries, the table is divided into more pages.

Search Form

At the top of the page there is a search form, where you can enter values to restrict the output. The meaning of each attribute is described below. Some attributes are only available for the List tab.



Interval: 1 hour ago
From: 2020-05-04 10:04
To: 2020-05-04 11:04

- Advanced search

Identify device by: MAC address
IP address, subnet, or hostname:
User ID:
Sources: Click to add items
MAC address:
VLAN:
Host OS: – Unspecified –

Active devices search form

Interval - set interval of displayed data. Either select one of the preset segments or type in the desired date and time in the **From** and **To** fields.

Identify device by - this field allows to change the identification key of the active device. This choice can be applied for the search query only. A global settings of the device identification can be set in *Configuration Center → FMC Configuration → Active devices*.

IP address, subnet or hostname - field for search by IP address, subnet or hostname. It supports both IPv4 and IPv6. To display all IPv4 addresses insert string 0.0.0.0/0, for all IPv6 addresses 0::/0.

MAC address - field for search by MAC address.

User ID - this option will filter devices where user with provided ID was logged in. For this feature, collector must process syslog messages from identity services like DHCP servers, VPN, directory services etc.

VLAN - search can be limited by the VLAN value. It displays only the devices that communicated in the virtual network.

Sources - select relevant flow sources.

Host OS - the third line allows you to choose one of the operating systems that can be detected by Flowmon Probe for all HTTP client devices. For this feature, flow data must be exported by Flowmon Probe.

The following options are available for List tab only.

Limit to - limits the number of results that are displayed. For faster response, we recommend to reduce this value to the required limit. In case some rows are merged, the total row number is lower. See attribute below.

Merge flows with gap - database stores flows in manner they are always closed at the end of hour, i.e. one flow will be displayed on multiple lines if lasted longer than one hour. To merge these flows, you need to check this box. The second value you can set is the maximum time gap between flows that you want to join. It is set to 15 minutes by default. If some flows are merged, the number of records in the table is lower than the value of **Limit to**.

Aggregate - if you want an overall view of communication in the network, you can use this setting to merge records that have common characteristics. If you check the **IP address** value, records with the same listening port, VLAN and IP address will merge into one. If you check the **MAC address** value, records that have the same listening port, VLAN, and MAC address will merge into one. The same applies for **Host OS** and **User ID**. In the **First seen** column, time is displayed since when the device was active. In the **Last seen** column is the time until when the device was active.

Show routers - MAC addresses of routers are set in the Configuration Center. These devices change the MAC addresses in the packets, thus these MAC addresses are assigned to many different IP addresses. In order to show result as clearly as possible, router records are not shown in the table. If you wish to see them, check this field.

View button - Click on this button to perform the query according to configured parameters. The result will be listed in the results table.

Export to CSV button - to save the search result to CSV file, click on this button. It executes the query and after a while it will offer you to download the generated file.

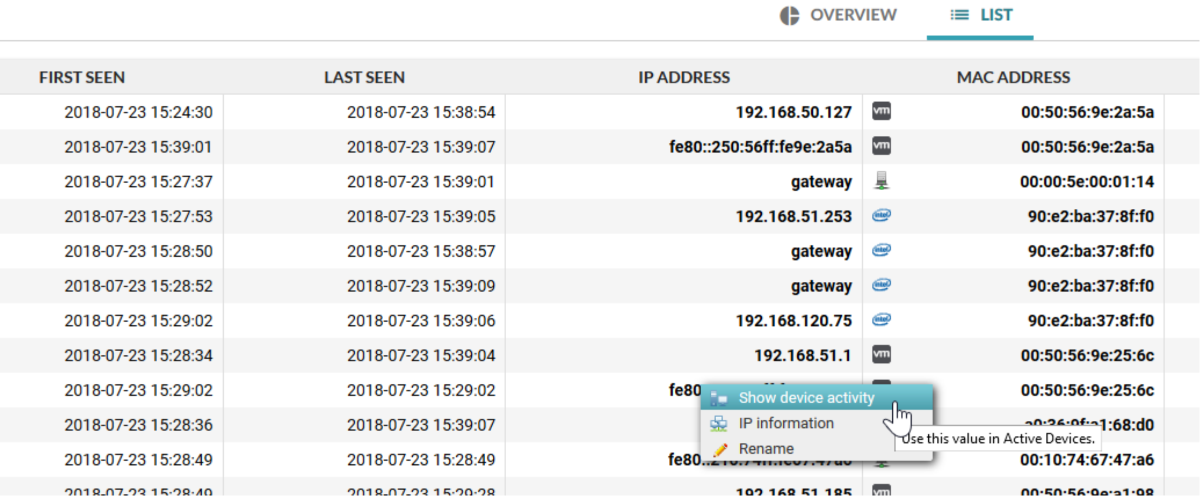
Export to PDF button - executes the query and generates PDF file for download.

Overview Tab

After entering the search criteria and pressing the **View** button under the form, the widgets will be shown. In the widgets various useful information is displayed. The widgets can be used in Flowmon Dashboard module as well.

List tab

After entering the search criteria and pressing the **View** button under the form, the table with the results will be shown. Number of table columns may vary according to merging. In the **First seen** column is shown the date and time when the device started to communicate. In the **Last seen** column is shown the time when communication was stopped. The **IP address** column shows the IP address of the device at that time. Column **MAC address** displays the MAC address of the device and manufacturer if the user has activated the **Resolve domain names** function. Columns **Host OS** and **User ID** displays more information, if available. The last two columns **VLAN** and **Flow source** display information about where the communication was intercepted.



FIRST SEEN	LAST SEEN	IP ADDRESS		MAC ADDRESS
2018-07-23 15:24:30	2018-07-23 15:38:54	192.168.50.127	vm	00:50:56:9e:2a:5a
2018-07-23 15:39:01	2018-07-23 15:39:07	fe80::250:56ff:fe9e:2a5a	vm	00:50:56:9e:2a:5a
2018-07-23 15:27:37	2018-07-23 15:39:01	gateway		00:00:5e:00:01:14
2018-07-23 15:27:53	2018-07-23 15:39:05	192.168.51.253	intel	90:e2:ba:37:8f:f0
2018-07-23 15:28:50	2018-07-23 15:38:57	gateway	intel	90:e2:ba:37:8f:f0
2018-07-23 15:28:52	2018-07-23 15:39:09	gateway	intel	90:e2:ba:37:8f:f0
2018-07-23 15:29:02	2018-07-23 15:39:06	192.168.120.75	intel	90:e2:ba:37:8f:f0
2018-07-23 15:28:34	2018-07-23 15:39:04	192.168.51.1	vm	00:50:56:9e:25:6c
2018-07-23 15:29:02	2018-07-23 15:29:02	fe80		00:50:56:9e:25:6c
2018-07-23 15:28:36	2018-07-23 15:39:07			1:68:d0
2018-07-23 15:28:49	2018-07-23 15:28:49	fe80		00:10:74:67:47:a6
2018-07-23 15:28:49	2018-07-23 15:29:28	192.168.51.185	vm	00:50:56:9e:a1:98

List of active devices

If you right click on the IP or MAC address field, context menu will appear in which you can rename these items or restrict the search by this value. At MAC address field there is also menu item **Add to a list of routers**, which stores the value in the routers table, that are not displayed in the results by default. If you have routers displayed and device is stored in the router table, item **Remove from router list** is displayed in the menu.

The footer of the table shows the summary of the total number of records displayed, the number of unique MAC addresses, IPv4 addresses and IPv6 addresses.

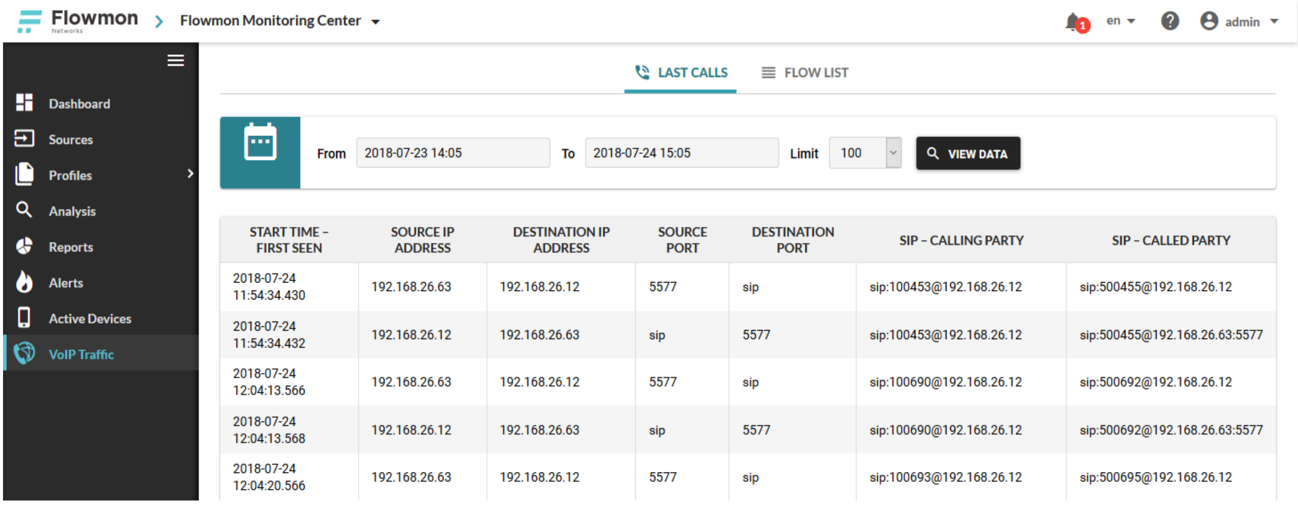
VOIP Traffic

Flowmon device supports VOIP traffic analysis and detection of its most important characteristics. For monitoring of this traffic, the Flowmon Networks proprietary technology is used, so only flow data from Flowmon Probe are supported. IPFIX protocol must be used. For enabling of this functionality, it is necessary to activate it on both probe on the Monitoring ports page and collector on page FMC Configuration.

Probe can recognize packets of protocols SIP, RTP and RTCP and stores information from these packets into flows. For SIP protocol it can be e.g. service communication (call initialization, accept, reject, termination, etc.). For protocol RTP it can be e.g. used codec and for protocol RTCP information about quality of call. Information about quality obtained from RTCP protocol is complemented with the same information based on probe measurements. For correlated SIP/RTP/RTCP information, Flowmon Probe must be configured to use the Extended VoIP option.

Last Calls Tab

In this tab all calls detected in selected time interval are shown. These calls where reconstructed from VOIP flows. Incomplete calls are also listed.

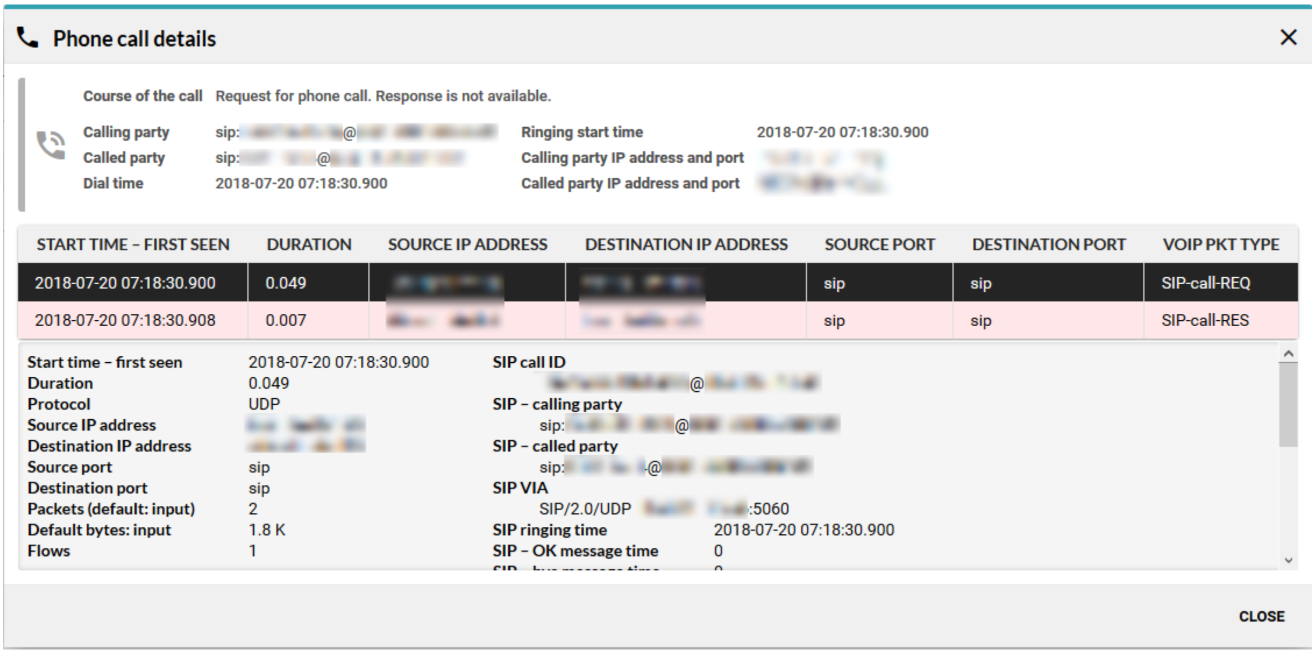


From 2018-07-23 14:05 To 2018-07-24 15:05 Limit 100

START TIME - FIRST SEEN	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	SOURCE PORT	DESTINATION PORT	SIP - CALLING PARTY	SIP - CALLED PARTY
2018-07-24 11:54:34.430	192.168.26.63	192.168.26.12	5577	sip	sip:100453@192.168.26.12	sip:500455@192.168.26.12
2018-07-24 11:54:34.432	192.168.26.12	192.168.26.63	sip	5577	sip:100453@192.168.26.12	sip:500455@192.168.26.63:5577
2018-07-24 12:04:13.566	192.168.26.63	192.168.26.12	5577	sip	sip:100690@192.168.26.12	sip:500692@192.168.26.12
2018-07-24 12:04:13.568	192.168.26.12	192.168.26.63	sip	5577	sip:100690@192.168.26.12	sip:500692@192.168.26.63:5577
2018-07-24 12:04:20.566	192.168.26.63	192.168.26.12	5577	sip	sip:100693@192.168.26.12	sip:500695@192.168.26.12

List of reconstructed calls

By clicking on call, a dialog box with call details is opened. It shows information about calling and called parties, call times, used codecs, call quality (reported by RTCP and measured by probe) etc.



Course of the call: Request for phone call. Response is not available.

Calling party: sip:[redacted]@[redacted]
Called party: sip:[redacted]@[redacted]
Dial time: 2018-07-20 07:18:30.900
Ringing start time: 2018-07-20 07:18:30.900
Calling party IP address and port: [redacted]
Called party IP address and port: [redacted]

START TIME - FIRST SEEN	DURATION	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	SOURCE PORT	DESTINATION PORT	VOIP PKT TYPE
2018-07-20 07:18:30.900	0.049	[redacted]	[redacted]	sip	sip	SIP-call-REQ
2018-07-20 07:18:30.908	0.007	[redacted]	[redacted]	sip	sip	SIP-call-RES

Start time - first seen	2018-07-20 07:18:30.900
Duration	0.049
Protocol	UDP
Source IP address	[redacted]
Destination IP address	[redacted]
Source port	sip
Destination port	sip
Packets (default: input)	2
Default bytes: input	1.8 K
Flows	1

SIP call ID
[redacted]@[redacted]
SIP - calling party
sip:[redacted]@[redacted]
SIP - called party
sip:[redacted]@[redacted]
SIP VIA
SIP/2.0/UDP [redacted]:5060
SIP ringing time 2018-07-20 07:18:30.900
SIP - OK message time 0

Call details

RTP jitter is measured in RTP timestamp units. RTP timestamp unit is based on the sampling rate. For example, for the sampling rate of 8000 Hz (PCMA) one unit is equal to 1/8000 of a second. For details, refer to RFC 3550 - interarrival jitter.

Flow List Tab

In this tab all monitored VOIP flows for the selected time interval are shown. The rows have specific color according to the detected protocol. By clicking on the link in the VOIP PKT TYPE column, the reconstruction of the whole call is performed and the dialog box with call details is shown (the same as in Last calls tab).

Flowmon Dashboard and Reports

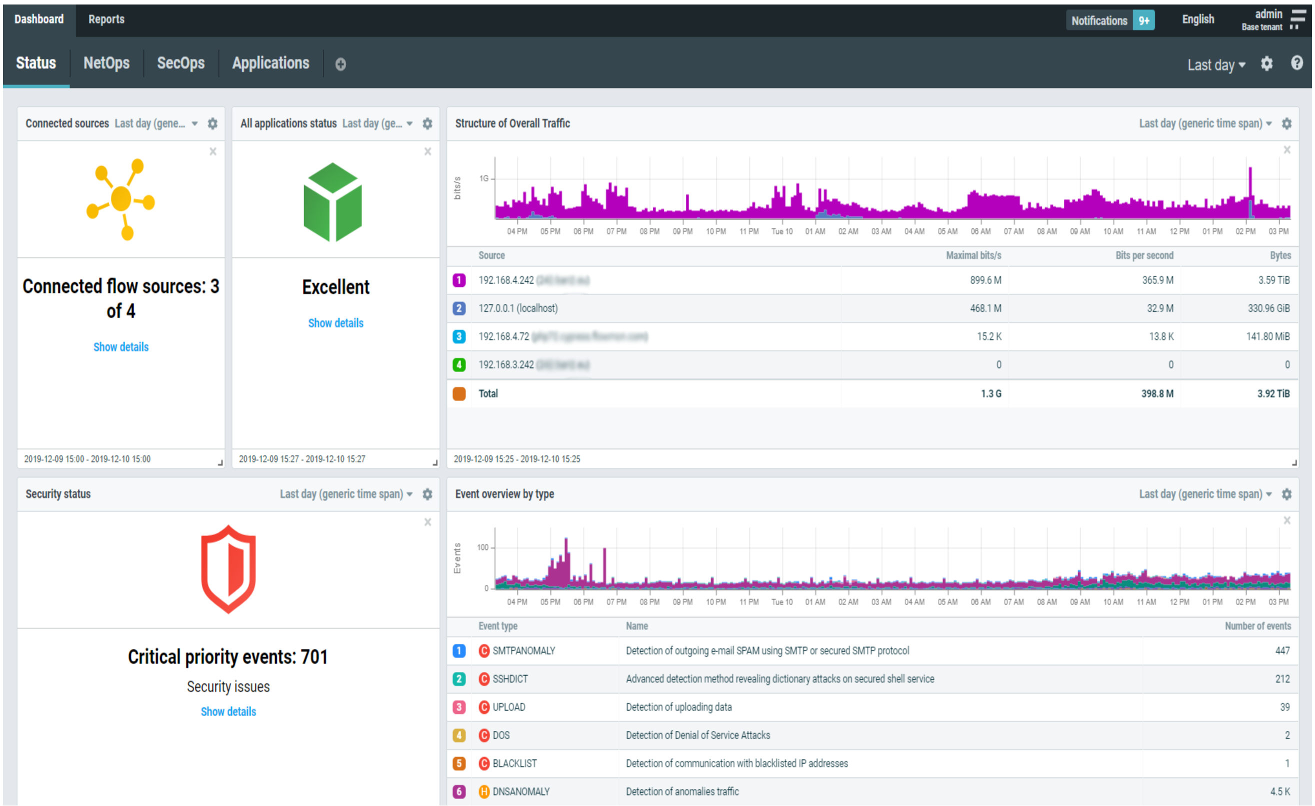
This section consists of the Dashboard and the Report. The following chapters describe their functionalities.

- Dashboard
    - Creating and Editing Dashboards
    - Widgets
    - User Menu
- Reports
    - Reports Tab
    - Schedules Tab
    - Chapters Tab
- Configuration
    - Presets
    - Topologies
- General
    - Notifications
    - Table Functionalities

Dashboard

Flowmon Dashboard (FMD) displays all widgets from other Flowmon modules in one place. Each user can define multiple dashboard tabs for their own set of widgets and thus focus on their points of interest that are located in various Flowmon modules. User may switch between different dashboards at the top of page.

Each widget queries the data from its parent module. Users can see only the data from the module they have permissions for.



Connected flow sources: 3 of 4

2019-12-09 15:00 - 2019-12-10 15:00

Excellent

2019-12-09 15:27 - 2019-12-10 15:27

	Source	Maximal bits/s	Bits per second	Bytes
1	192.168.4.242 [redacted]	899.6 M	365.9 M	3.59 TiB
2	127.0.0.1 (localhost)	468.1 M	32.9 M	330.96 GiB
3	192.168.4.72 [redacted]	15.2 K	13.8 K	141.80 MiB
4	192.168.3.242 [redacted]	0	0	0
🟧	**Total**	**1.3 G**	**398.8 M**	**3.92 TiB**

2019-12-09 15:25 - 2019-12-10 15:25

Critical priority events: 701

Security issues

	Event type	Name	Number of events
1	C SMTPANOMALY	Detection of outgoing e-mail SPAM using SMTP or secured SMTP protocol	447
2	C SSHDICT	Advanced detection method revealing dictionary attacks on secured shell service	212
3	C UPLOAD	Detection of uploading data	39
4	C DOS	Detection of Denial of Service Attacks	2
5	C BLACKLIST	Detection of communication with blacklisted IP addresses	1
6	H DNSANOMALY	Detection of anomalies traffic	4.5 K

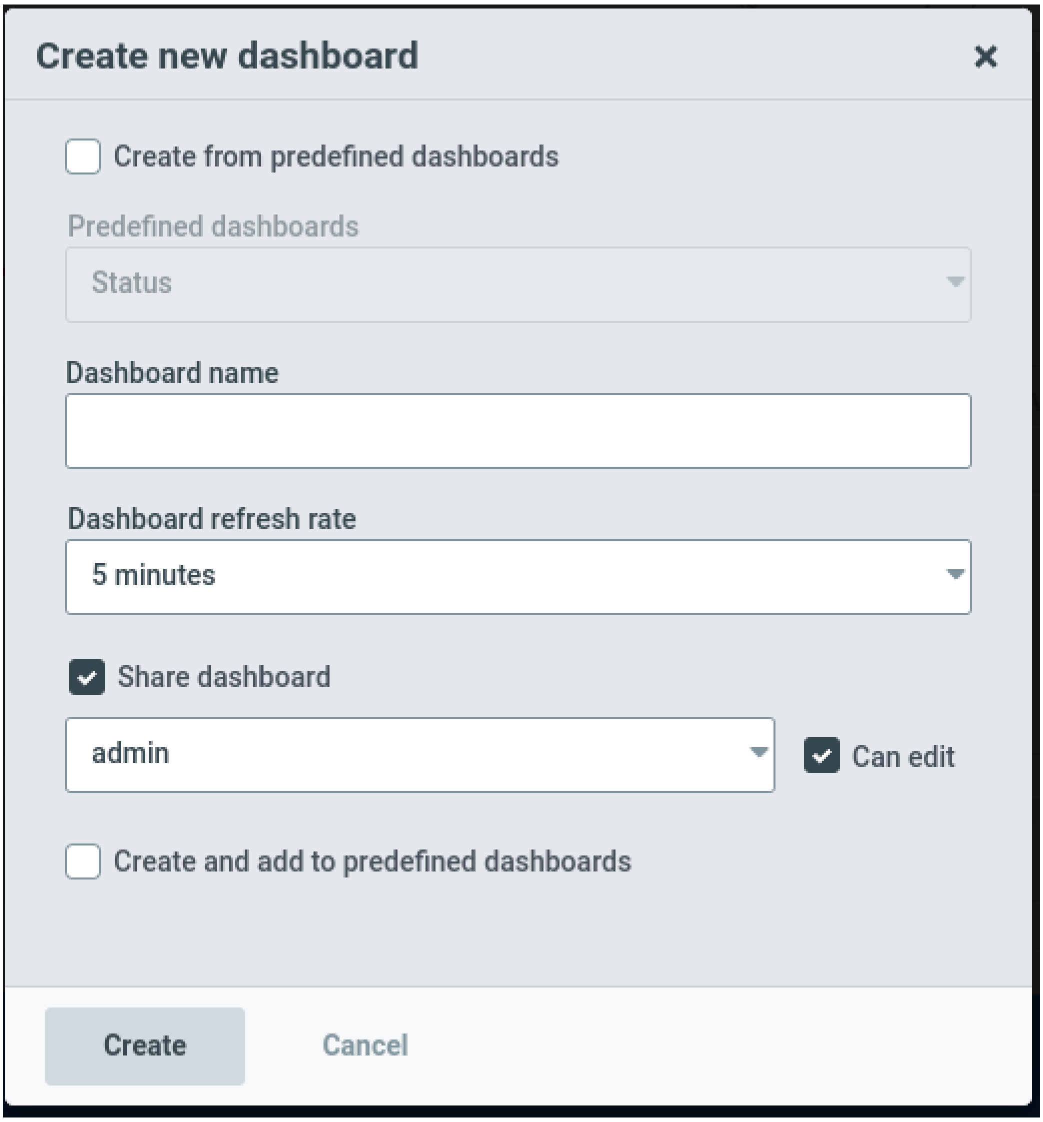
Dasboard - Overview

Creating and Editing Dashboards

New dashboard can be created by clicking on the + button in the upper menu. In order to display the widgets, at least one dashboard has to be created.

Create dashboard

A dashboard can be can created as new blank dashboard or from the list of predefined dashboards. When creating the dashboard, name, refresh rate (how often will be refreshed) and list of groups and users in section Share dashboard. For shared dashboards, a check-box "Can edit" can be used to allow roles and users to make changes in the dashboard.


Create new dashboard

□ Create from predefined dashboards

Predefined dashboards: Status

Dashboard name:

Dashboard refresh rate: 5 minutes

☑ Share dashboard

admin ☑ Can edit

□ Create and add to predefined dashboards

Predefined dashboards

User can either create an empty dashboard or create a ready-to-use dashboard from the list of predefined dashboards (the list reflects installed modules and predefined dashboards from other users within the same tenant). When creating a new dashboard from the predefined dashboards, the widgets are automatically created and the user can adjust their settings, remove them, add other widgets or customize their position on the dashboard. User must have permission for adding dashboard into predefined dashboards. Predefined dashboards include:

- Predefined by Flowmon
    - the Status dashboard - top level dashboard that combines information from Monitoring Center, Flowmon ADS and Flowmon APM.
    - the NetOps dashboard - creates a dashboard with widgets focused on the Network Operations use cases.
    - the SecOps dashboard - creates a dashboard with widgets focused on the Security Operations use cases (requires also Flowmon ADS module).
    - the Applications dashboard - creates a dashboard with widgets focused on Application Performance Monitoring (requires also Flowmon APM module).
- Predefined by users - creates a dashboard which was set as predefined by other users.

Edit dashboards

Dashboards can be edited by clicking on the ⚙ button in the upper menu.

Dashboard settings allow to manage dashboard tabs and their settings. It is possible to re-order the dashboards (only in My dashboards section), edit a dashboard, delete a dashboard or create a new one. "Create new report" option converts a dashboard tab into a report. A pre-filled form for creation of reports (name and chapters are pre-filled, an example form is available at this page).

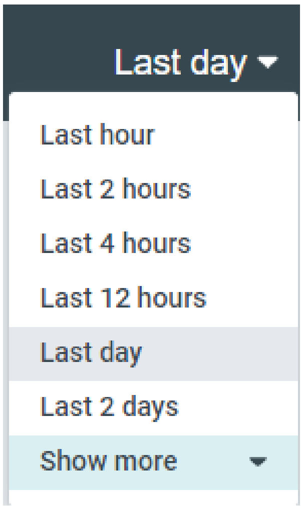
There are two sections of dashboards - My dashboards and Hidden. Hidden section is used for dashboards which we do not want to see among the tabs. This feature is handy especially when someone shares a dashboard with the user who does not want to use the shared dashboard. Switch between *My dashboards* and *Hidden dashboards* can be done both via the menu and drag&drop.

A dashboard status shows the sharing information. Private (just the user), Shared (shared with other roles or users) and Shared with me (another users shared a dashboard with me).

When editing a dashboard, it can be added to predefined. It will appear in the list of predefined dashboards for the other users and they can create a copy of the dashboard and customize it for themselves.

Global Time Interval

The upper part of the page includes a list box that allows to change the time interval for the all widgets in the dashboard. The time interval is by default set to the last day. The selected interval will be applied to all widgets in the dashboard, unless the widget has its own interval settings.



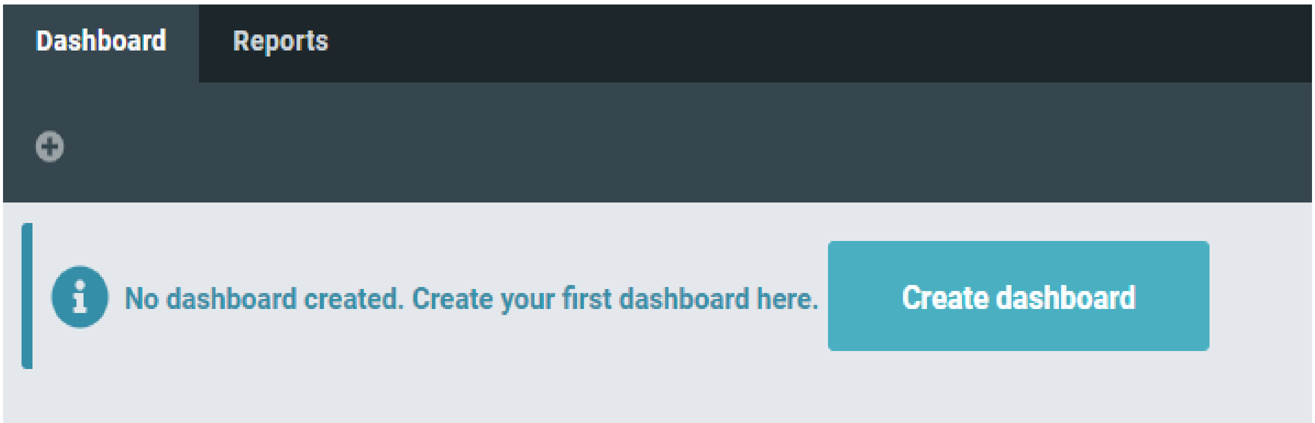
Widgets

- Initial Creation of Widgets
- Widget Detail
- Adding New Widgets
    - Category selection
    - Data to display selection
    - Widget name
    - Data range
    - Widget settings
- Widget Settings Detail
    - Pie chart
    - Summary pie chart

  - Table
  - Time series chart
  - Summary
  - Topology visualization
  - Data settings
- Status widgets
- Topology Widget

Initial Creation of Widgets

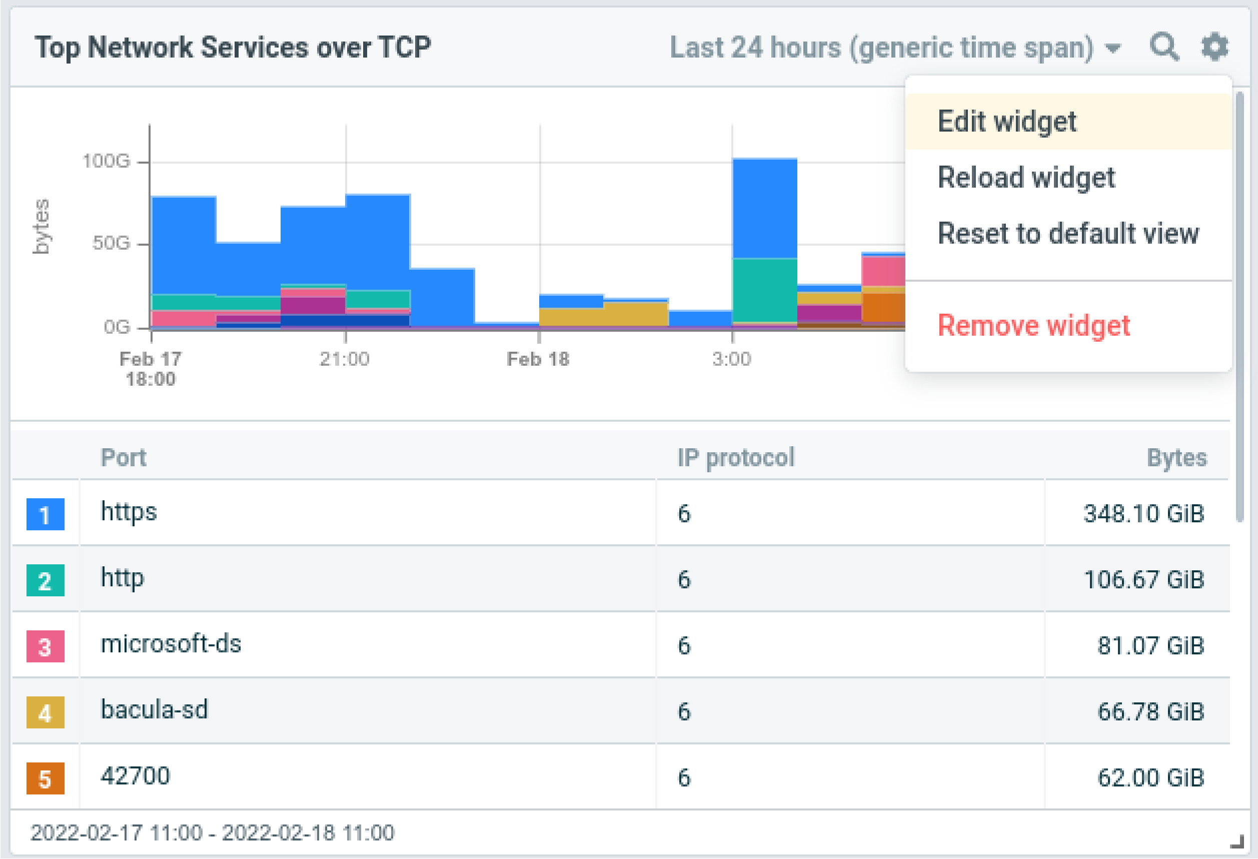
When viewing the Dashboard and Reports section for the first time, the user will find this section empty. Creation of a default dashboard is available by clicking the respective button. For further details please steps in Creating and Editing Dashboards.



No dashboard created. Create your first dashboard here.

Create dashboard

Widget Detail



Top Network Services over TCP

	Port	IP protocol	Bytes
1	https	6	348.10 GiB
2	http	6	106.67 GiB
3	microsoft-ds	6	81.07 GiB
4	bacula-sd	6	66.78 GiB
5	42700	6	62.00 GiB

2022-02-17 11:00 - 2022-02-18 11:00

Each widget can be adjusted by:

- Resizing the widget
- Changing the position of the widget
- Change the widget data selection

Clicking the setting icon opens additional menu, which consists of:

- **Edit widget** - Displays widget settings dialog. This dialog can be used to modify widget settings. For more details see the section adding new widget.
- **Reload widget** - Will refresh widget immediately. Apart from immediate (on demand) refresh, all widgets in dashboard are refreshed periodically after a set interval. This interval can be changed in widget header (for a specific widget) or in dashboard upper menu (default interval for all widgets in dashboard).
- **Reset to default view** - Restores default widths of columns in displayed table.
- **Remove widget** - Removes the widget from the dashboard.

Clicking the magnifier icon opens new browser tab displaying current widget-data in its parent module. In parent module, user is free to take any further actions to analyze the data.

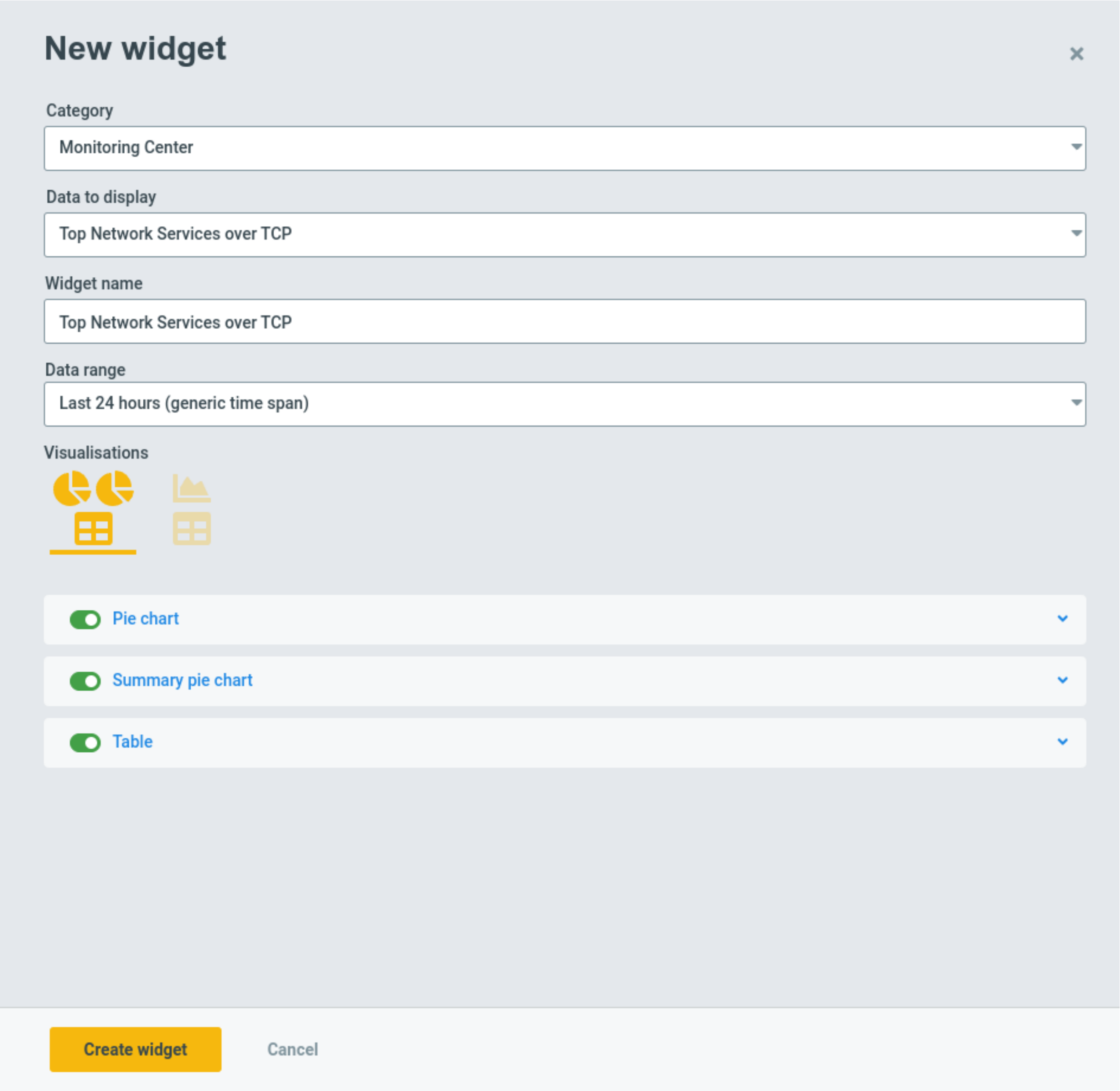
Adding New Widgets

It is possible to add new widget by clicking the **New widget** button.

New widget button

This dialog can be used for adding a new widget or changing settings of existing widget. The dialog consists of five main groups of settings:

- Category
- Data to display
- Widget name
- Data range
- Widget settings



New widget

Category: Monitoring Center

Data to display: Top Network Services over TCP

Widget name: Top Network Services over TCP

Data range: Last 24 hours (generic time span)

Visualisations

Category selection

Displays list of categories (modules) that offer the widgets which can be added to the dashboard.

Data to display selection

This selection is populated in accordance with the content of the Category selection. The user may select the data endpoints available for the respective category.

Widget name

Can be used to customize widget name. The default value is the same as Data to display selection.

Data range

Defines the interval for which the data will be displayed. By default, this option uses the general time interval (available in the top-right corner).

It is possible to select the following data range:

- Last hour
- Last 2 hours
- Last 4 hours
- Last 12 hours
- Last 24 hours
- Last 2 days
- Last 4 days
- Last 7 days
- Last 2 weeks
- Last 4 weeks
- Last 3 months

Widget settings

Each data endpoint offers various kinds of data. Dashboard offers one or more widget types that are the most suitable for visualizing such data.

Each widget may be composed of various elements:

- Table
- Pie chart
- Time series chart

Depending on the selected category, displayed data and selected widget type, this elements can be enabled or disabled.

Widget Settings Detail

Different types of widget are represented by variety of interactive icons. User can turn on/off a visualization by clicking the respective icon.

Sample widget icon:

Pie chart and table

Selecting a widget type allows the user to configure further settings:

Pie chart

- **Metric** - allows to choose one of the available metrics, which will serve as a base for the pie chart. The metric is also presented in the table which serves as a chart legend.

- **Chart description** - allows to label the pie chart slices with one of the available parameters. The parameter consist of the description of the respective metric.
- **Summaries** - contains a list of all available summary values that are present in the data endpoint of a pie chart. Any of the summary values can be selected to be displayed in the chart.

Summary pie chart

- **Metric** - allows to choose one of the available metrics, which will serve as a base for the pie chart. The metric is also represented in the form of a number in the table which serves as a chart legend.
- **Summaries** - contains a list of all available summary values that are present in the data endpoint of a pie chart. Any of the summary values can be selected to be displayed in the chart.

Table

- **Show colors** - if enabled, an extra column containing a color legend is added to the table.
- **Show percents** - some widget types support showing percentage values in the table.
- **Columns** - contains a list of all available table columns that are present in the chapter. User can select any of the columns to be displayed in the table.
- **Summaries** - contains a list of all available summary table rows that are present in the chapter. User can select any of the rows to be displayed in the table.

Time series chart

- **Series** - contains a list of all time series that are present in the data endpoint. Any list of them can be selected for display in the chart.
- **Stacked chart** - displays time series stacked on top of each other.
- **Axis** - allows to choose between the linear and logarithmic axis.

Summary

- **Columns** - contains a list of all columns, which consist of different types of available information, that are present in the chapter. User can select any of the columns to be displayed.

Topology visualization

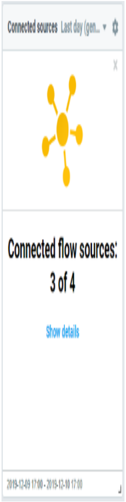
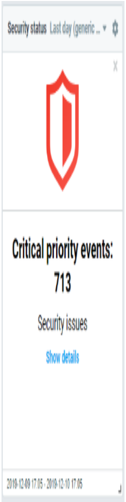
- **Opacity** - for topologies you can set opacity for map. It is available for the map type topology only.

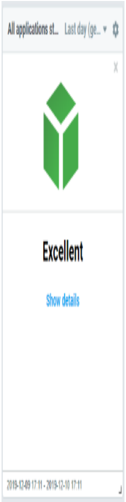
Data settings

- Depending on a data endpoint, other data search parameters might be available for configuration
- The settings are displayed in a table containing the following columns:
  - **Name** - name of the parameter
  - **Show in the widget** - if checked, input field to set the parameter value will be displayed in the widget
  - **Use default** - if checked, default values will be used
  - **Custom value**

- if the "use default" is not checked, custom value will be used instead
- depending on data endpoint, each parameter can accept either a value from allowed list displayed in a select box, or an arbitrary value

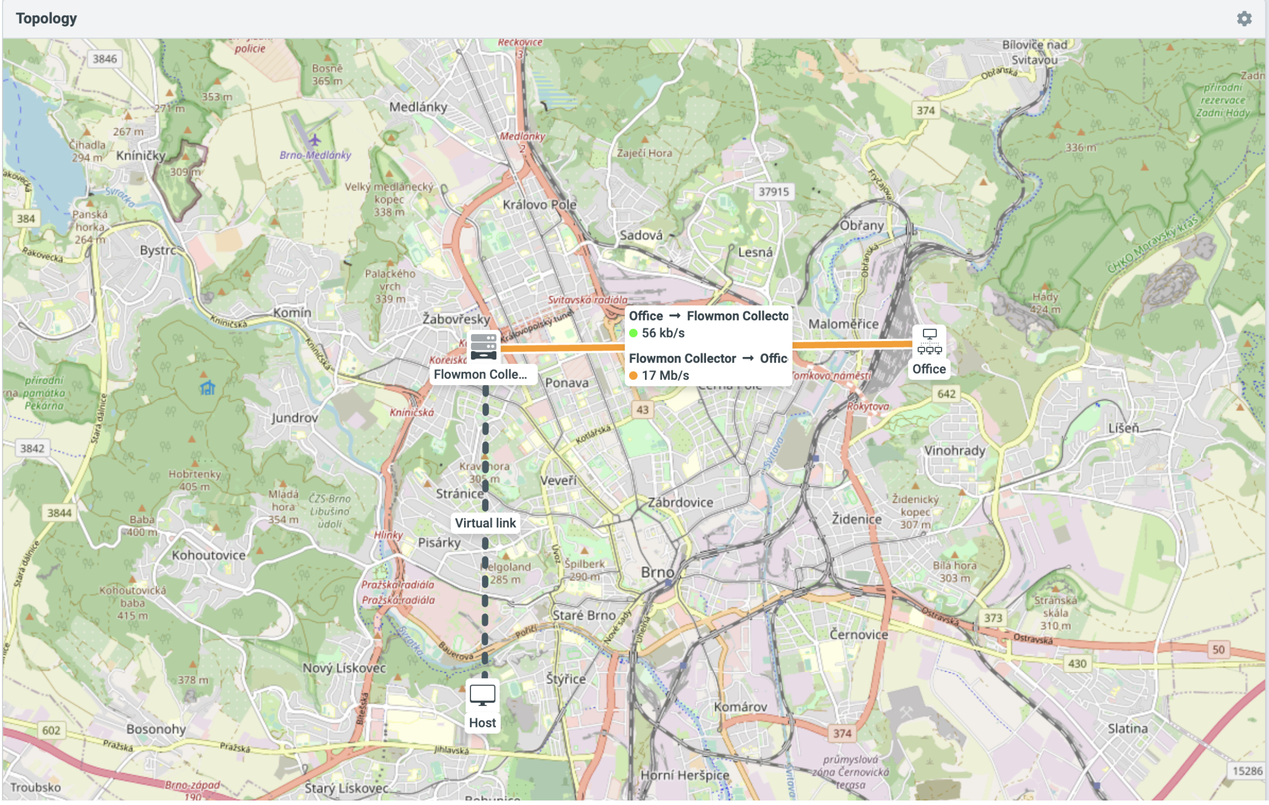
Status widgets

Widget	Description
 Connected sources Last day (gen... ▾ ⚙ Connected flow sources: 3 of 4 Show details 2019-12-09 17:00 - 2019-12-10 17:00 Connected sources	Widget represents connected nodes like “networks” or sources of the flow data. A source is considered to be connected if some data was received from it within the previous 5 minute interval. Widget color signals how many of sources are connected: • Green - everything works well (>= 75% sources connected) • Yellow - minor issues detected (< 75% sources connected) • Orange - major issues detected (< 50% sources connected) • Red - critical issues detected (< 25% sources connected)
 Security status Last day (generic ... ▾ ⚙ Critical priority events: 713 Security issues Show details 2019-12-09 17:05 - 2019-12-10 17:05	Security status is represented by a shield showing different colors as per the selected perspective and events within that perspective in Flowmon ADS. The number of events in highest detected category can also be shown. The status of a widget is manifested by a color: • Green - no events or information level events detected • Yellow - low priority events detected • Orange - medium priority events detected • Light red - high priority events detected • Dark red - critical events detected The “Show details” section provides name of the perspective and number of events in individual levels of severity.

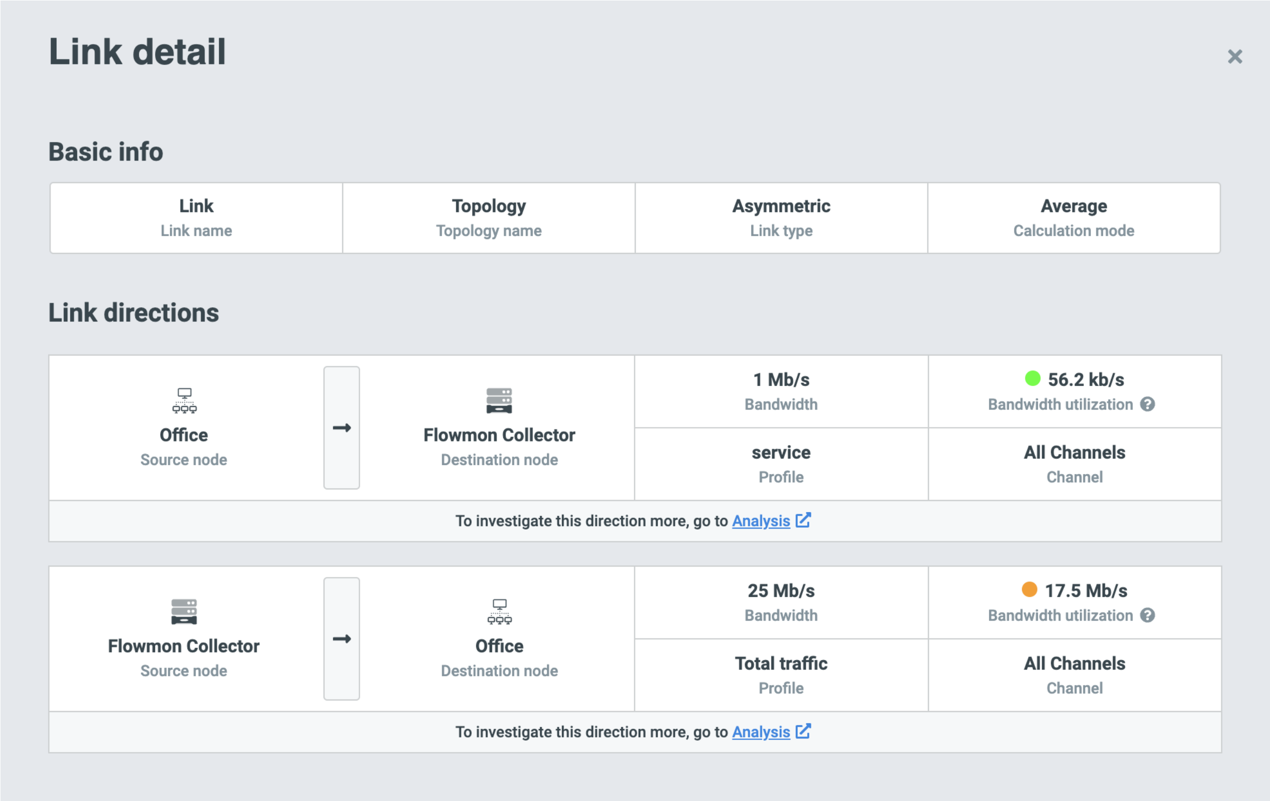
Widget	Description
 All applications st... Last day (ge... ▾ Excellent Show details 2019-12-09 17:11 - 2019-12-10 17:11	Application status widget is based on APM Index calculated for all applications within selected time frame. It requires Flowmon APM. The overall status represents a weighted average for monitored applications. So if some application has very poor APM index, but the number of transactions is low, it does not necessarily affect the overall status. Four different colors represent different values of the APM Index: • Green - everything ok, index > 90 • Yellow - minor issues, index > 80 • Orange - major issues, index > 70 • Red - critical situation, index <=70

Topology Widget

All topologies can be used as widgets on a dashboard or as a chapter in a report. From the report it can be exported to PDF. Information about topologies is not available in the CSV format.



A link detail for a drill down is available when clicking the link in the widget or chapter. There, overview information about traffic in the link is available along with data charts for selected time span of the report or widget.



Link detail

×

Basic info

Link	Topology	Asymmetric	Average
Link name	Topology name	Link type	Calculation mode

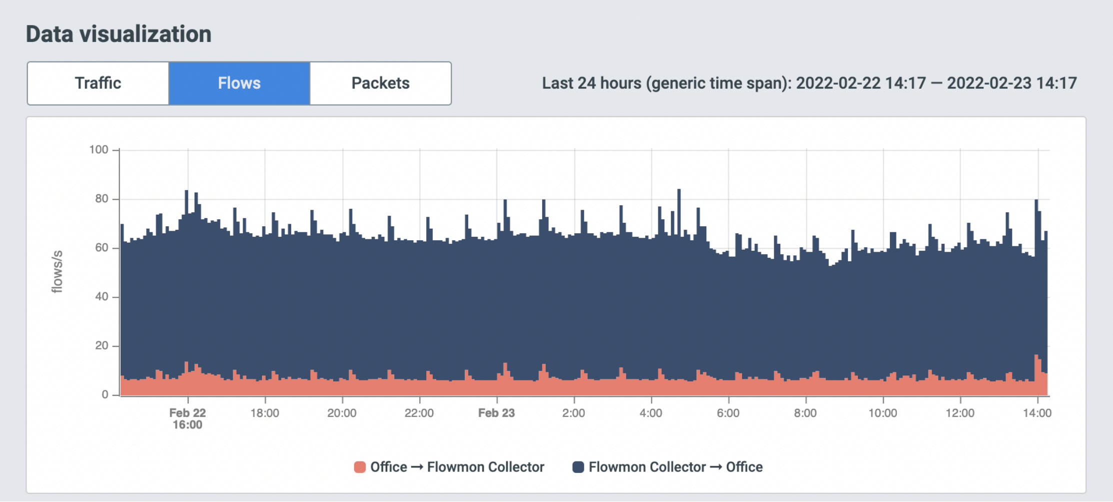
Link directions

Office Source node	→	Flowmon Collector Destination node	1 Mb/s Bandwidth	● 56.2 kb/s Bandwidth utilization ?
			service Profile	All Channels Channel

To investigate this direction more, go to Analysis

Flowmon Collector Source node	→	Office Destination node	25 Mb/s Bandwidth	● 17.5 Mb/s Bandwidth utilization ?
			Total traffic Profile	All Channels Channel

To investigate this direction more, go to Analysis



Data visualization

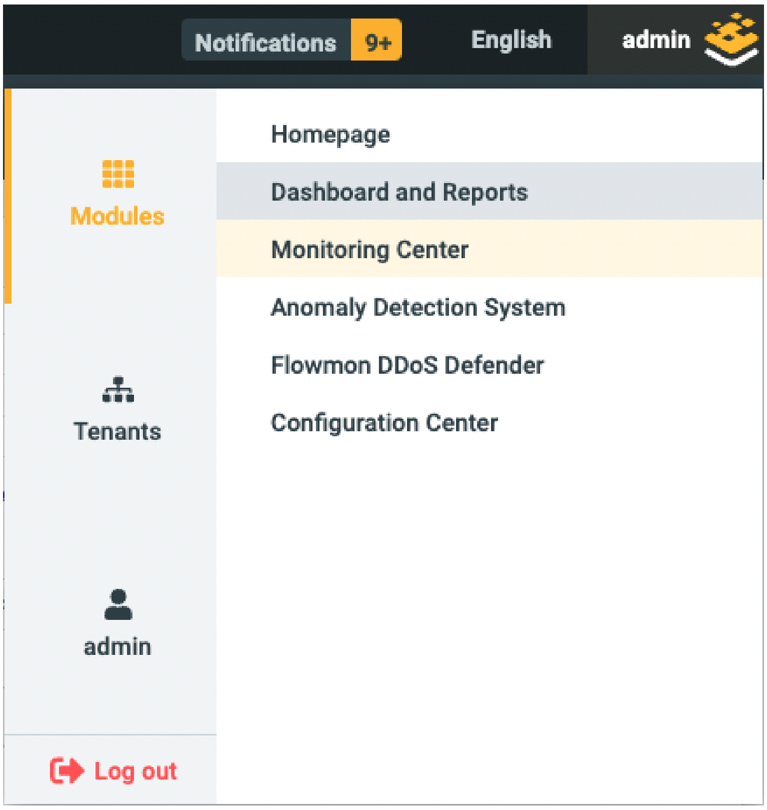
Traffic | Flows | Packets

Last 24 hours (generic time span): 2022-02-22 14:17 — 2022-02-23 14:17

User Menu

Clicking your username in the top right opens up a user menu with these items

- **Modules** - switch to a different Flowmon module
- **Tenants** - switch current tenant
- **Log out**



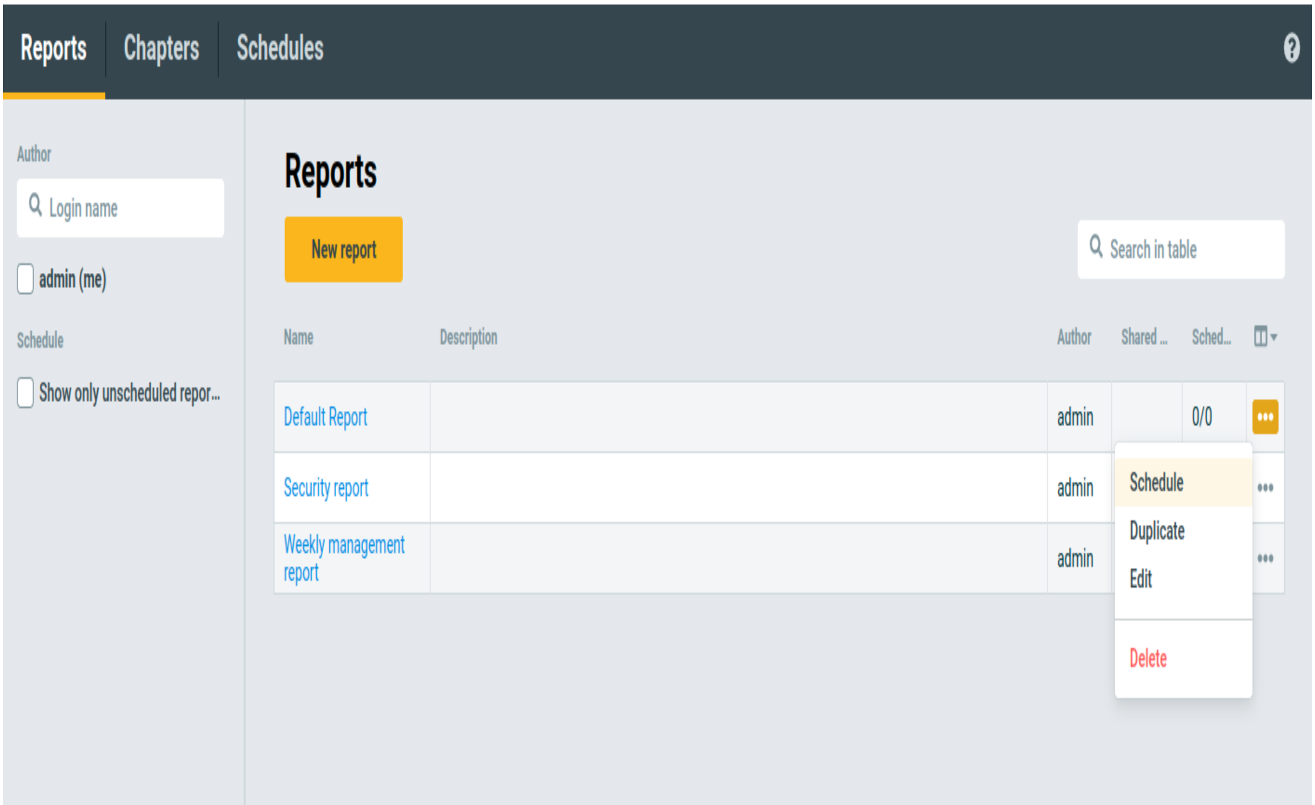
Reports

The Reports page displays reports from all Flowmon modules. You can create and schedule reports combining chapters from different modules. The page consists of the following tabs:

- Reports Tab
- Schedules Tab
- Chapters Tab

Reports Tab

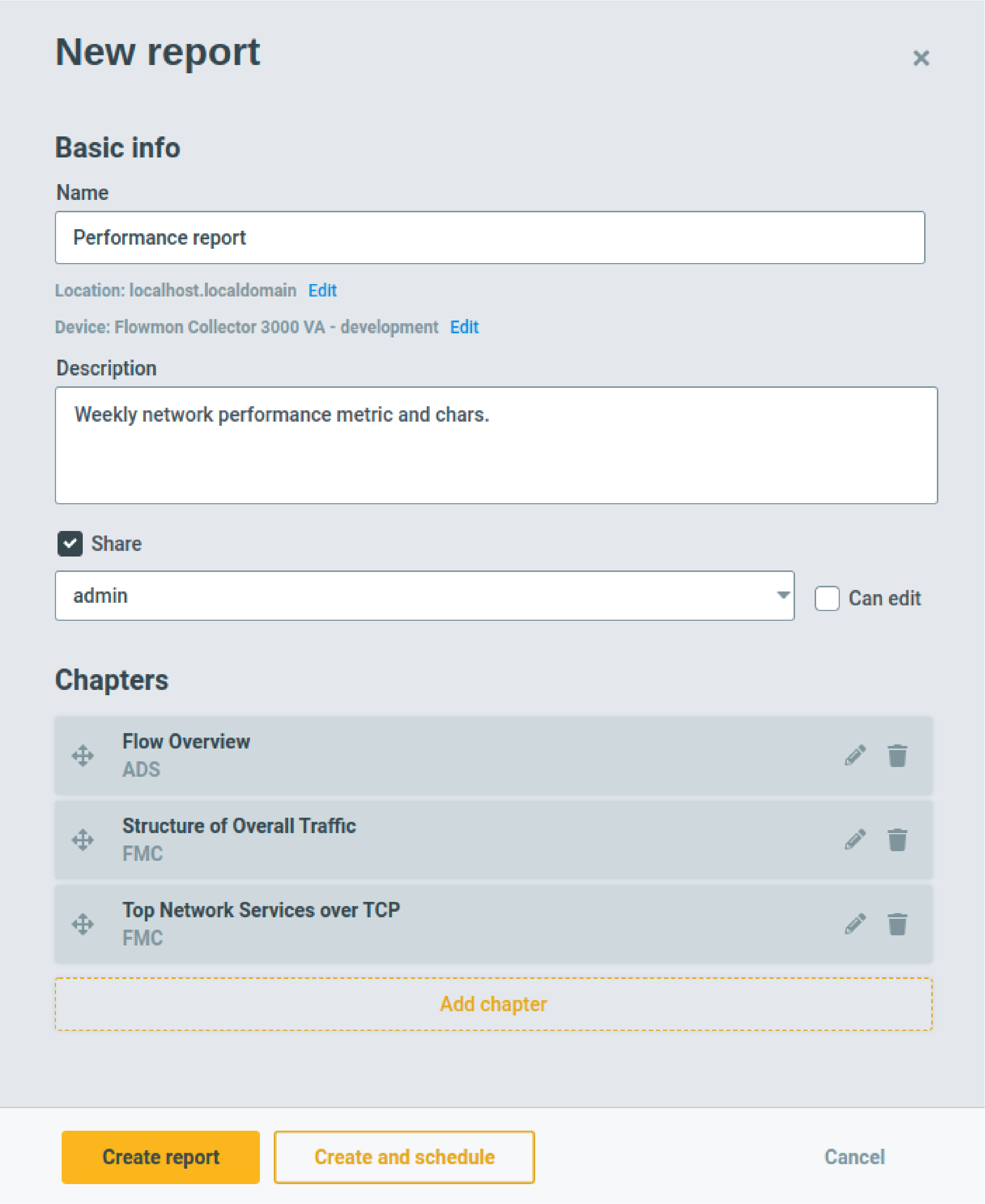
The Reports tab allows you to add and manage reports. A user with the admin role sees reports of all users. To filter the reports, use the left sidebar or the search box on the right. Click **(More actions)** to schedule, duplicate, edit, or delete a report. Click the report name to open it.



Name	Description	Author	Shared ...	Sched...
Default Report		admin		0/0
Security report		admin		
Weekly management report		admin		

Click **New report** to create a report:

1. Enter the report name.
2. Click **Edit** to change the **Location** or the **Device** of the report.
3. Specify the report description.
4. Check **Share** to share the report with a specific user or a group of users with a specific role. Check **Can edit** to let those users edit the report.
5. Click **Add chapter** to add one or more chapters to the report. You can reorder added chapters by dragging and dropping.
6. Click the **Pencil icon** to edit the chapter name, description, and visualization settings.
7. Click **Create report** to finish or **Create and schedule** to schedule the new report right away. See Schedules Tab for more details about sending reports automatically.



New report

Basic info

Name: Performance report

Location: localhost.localdomain Edit

Device: Flowmon Collector 3000 VA - development Edit

Description: Weekly network performance metric and chars.

☑ Share

admin

□ Can edit

Chapters

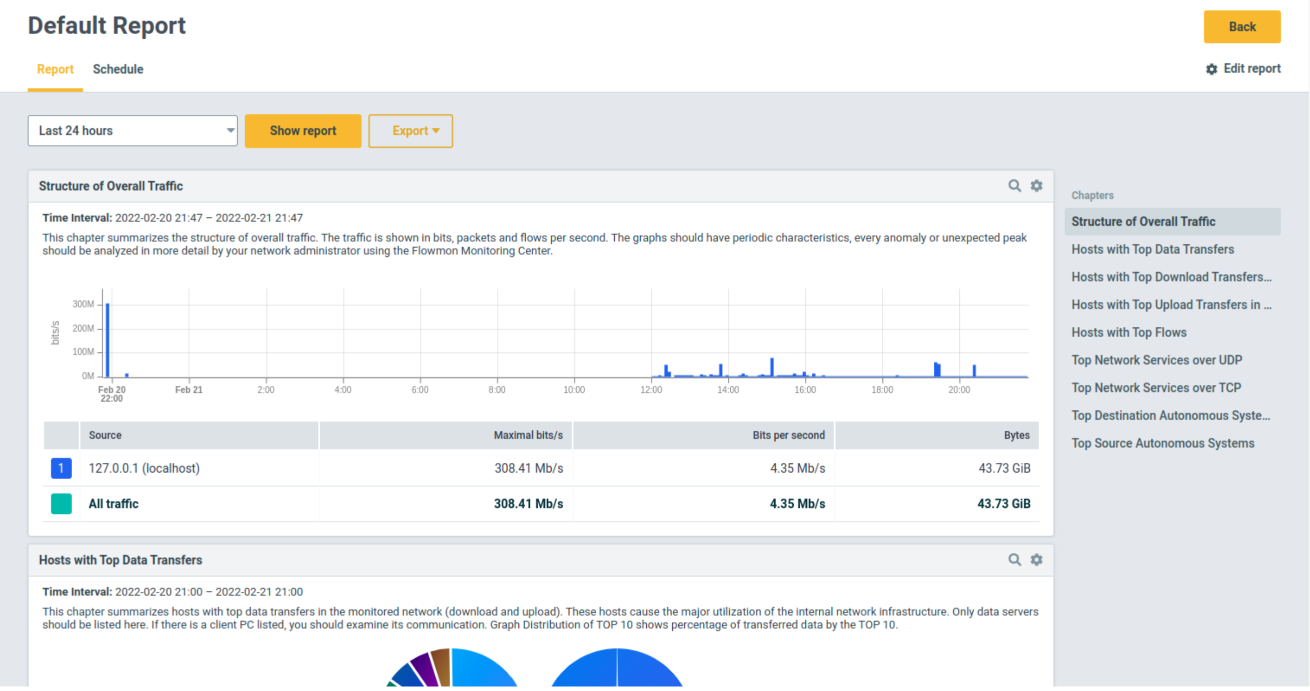
- Flow Overview — ADS
- Structure of Overall Traffic — FMC
- Top Network Services over TCP — FMC

Report Detail

The report detail displays data for each chapter in the report. You can jump to a specific chapter using the table of contents on the right.

Use the drop down menu in the top left to specify the report's time interval. Check **Apply working hours** to only include data from specific weekly time slots (see FMC Configuration/Working hours). Click **Show report** to apply the selected time interval and working hours. Click **Export** to save the report as a PDF or a CSV file.

The heading of each chapter contains icons for quick actions. Click the **Magnifying glass icon** to view the chapter data inside its module (for example, Monitoring Center or Anomaly Detection System). Click the **Gear icon** to edit the chapter settings.



Default Report
Back
Report
Schedule
Edit report
Last 24 hours
Show report
Export
Chapters
Structure of Overall Traffic
Hosts with Top Data Transfers
Hosts with Top Download Transfers...
Hosts with Top Upload Transfers in ...
Hosts with Top Flows
Top Network Services over UDP
Top Network Services over TCP
Top Destination Autonomous Syste...
Top Source Autonomous Systems
bits/s
300M
200M
100M
0M
Feb 20 22:00
Feb 21
2:00
4:00
6:00
8:00
10:00
12:00
14:00
16:00
18:00
20:00

Structure of Overall Traffic

Time Interval: 2022-02-20 21:47 – 2022-02-21 21:47

This chapter summarizes the structure of overall traffic. The traffic is shown in bits, packets and flows per second. The graphs should have periodic characteristics, every anomaly or unexpected peak should be analyzed in more detail by your network administrator using the Flowmon Monitoring Center.

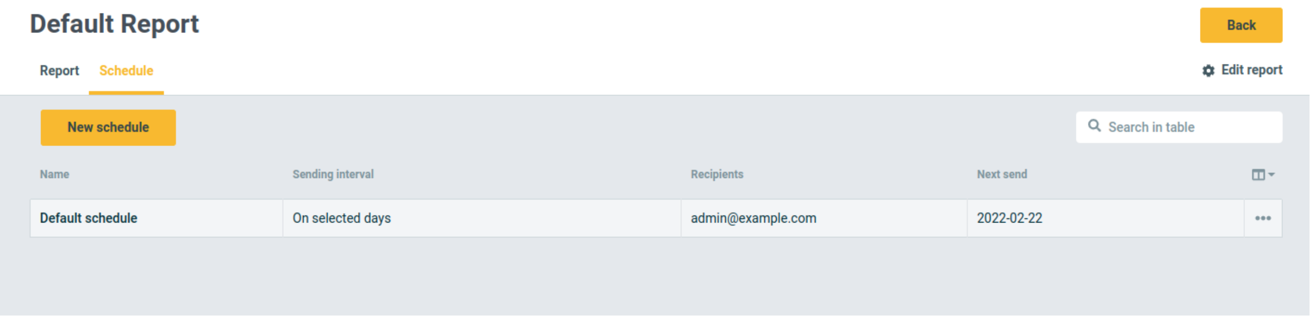
	Source	Maximal bits/s	Bits per second	Bytes
1	127.0.0.1 (localhost)	308.41 Mb/s	4.35 Mb/s	43.73 GiB
🟩	**All traffic**	**308.41 Mb/s**	**4.35 Mb/s**	**43.73 GiB**

Hosts with Top Data Transfers

Time Interval: 2022-02-20 21:00 – 2022-02-21 21:00

This chapter summarizes hosts with top data transfers in the monitored network (download and upload). These hosts cause the major utilization of the internal network infrastructure. Only data servers should be listed here. If there is a client PC listed, you should examine its communication. Graph Distribution of TOP 10 shows percentage of transferred data by the TOP 10.

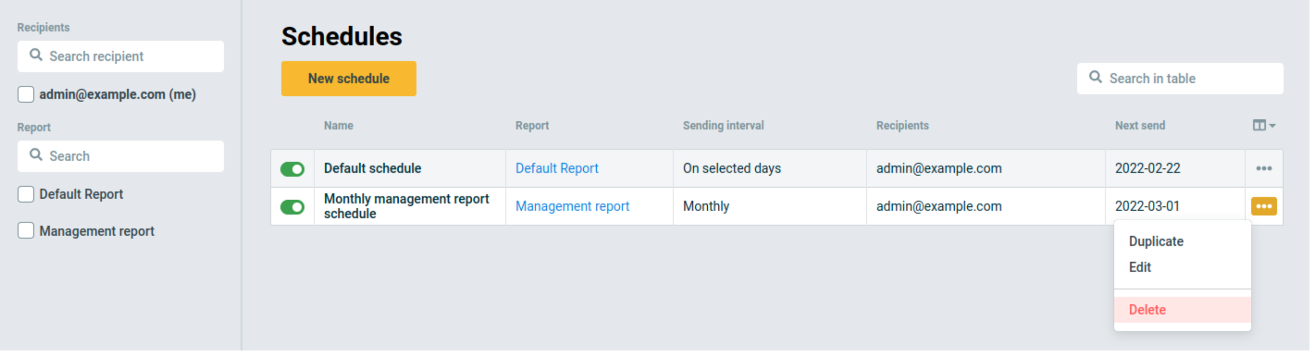
Switch to the **Schedule** tab to view the report's schedules. See Schedules Tab for more details about sending reports automatically.



Name	Sending interval	Recipients	Next send	
Default schedule	On selected days	admin@example.com	2022-02-22	•••

Schedules Tab

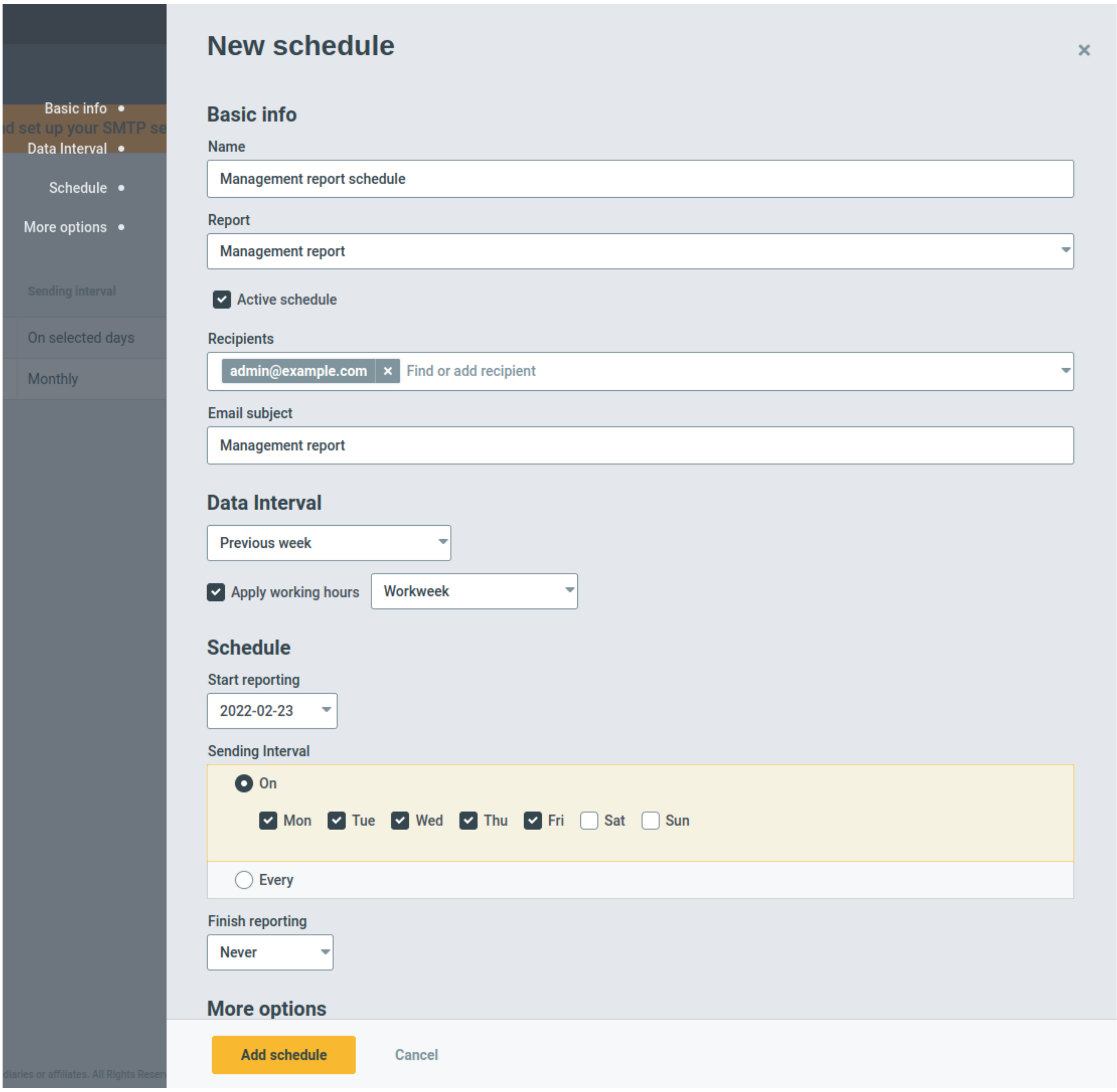
Schedules allow you to automate sending reports by email in regular intervals. In the **Schedules** tab, you can add and manage schedules. To filter your schedules, use the left sidebar or the search box on the right. Use the checkbox in the first column to enable or disable a schedule. Click **(More actions)** to duplicate, edit, or delete a schedule. Click the report name to open the scheduled report.



	Name	Report	Sending interval	Recipients	Next send	
●	Default schedule	Default Report	On selected days	admin@example.com	2022-02-22	•••
●	Monthly management report schedule	Management report	Monthly	admin@example.com	2022-03-01	•••

Click **New schedule** to create a schedule:

1. Enter the schedule name.
2. Select which report to send.
3. Keep **Active schedule** checked to activate the schedule right away.
4. Specify email addresses of the **Recipients**. Select from existing emails or add new ones.
5. Enter the email subject or click **Autofill the subject** to use the report name.
6. Select a **Data interval** for the report. For example, picking "Last 24 hours" means that the report will contain data from the 24 hours before it was sent.
7. Optionally, check **Apply working hours** to only include data from specific weekly time slots. See FMC Configuration /Working hours for more details.
8. Set the **Start reporting** date and the **Sending interval**. Optionally, you can also set a **Finish reporting** date.
9. Choose to send the report as a PDF or a CSV attachment (or both).
10. Pick the report language.
11. Optionally, you can send the report to an external storage server. See External storage for more details.
12. Optionally, check **Use GPG** to sign or encrypt the scheduled email (or both).
13. Finally, click **Add schedule**.



New schedule

Basic info

Name: Management report schedule

Report: Management report

☑ Active schedule

Recipients: admin@example.com × Find or add recipient

Email subject: Management report

Data Interval

Previous week

☑ Apply working hours: Workweek

Schedule

Start reporting: 2022-02-23

Sending Interval

● On

☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat □ Sun

○ Every

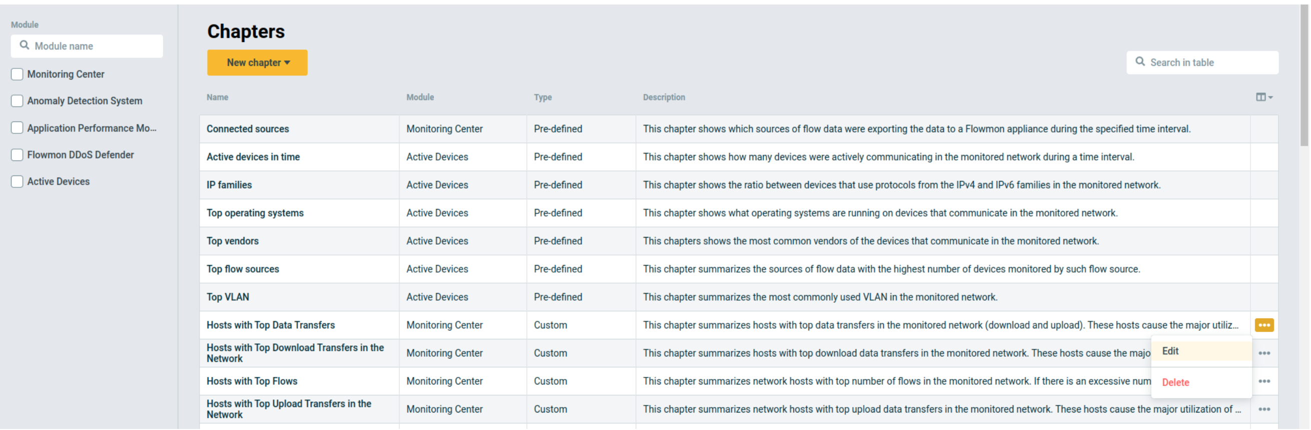
Finish reporting: Never

More options

Chapters Tab

The Chapters tab displays module chapters you can use as dashboard widgets or report chapters. To add a chapter to a report, use the Reports tab.

To filter the chapters, use the left sidebar or the search box on the right. Click ••• **(More actions)** to edit or delete a custom chapter. You cannot edit or delete predefined chapters. Click **New chapter** to create a chapter in one of the connected Flowmon modules.



Name	Module	Type	Description	
Connected sources	Monitoring Center	Pre-defined	This chapter shows which sources of flow data were exporting the data to a Flowmon appliance during the specified time interval.	
Active devices in time	Active Devices	Pre-defined	This chapter shows how many devices were actively communicating in the monitored network during a time interval.	
IP families	Active Devices	Pre-defined	This chapter shows the ratio between devices that use protocols from the IPv4 and IPv6 families in the monitored network.	
Top operating systems	Active Devices	Pre-defined	This chapter shows what operating systems are running on devices that communicate in the monitored network.	
Top vendors	Active Devices	Pre-defined	This chapters shows the most common vendors of the devices that communicate in the monitored network.	
Top flow sources	Active Devices	Pre-defined	This chapter summarizes the sources of flow data with the highest number of devices monitored by such flow source.	
Top VLAN	Active Devices	Pre-defined	This chapter summarizes the most commonly used VLAN in the monitored network.	
Hosts with Top Data Transfers	Monitoring Center	Custom	This chapter summarizes hosts with top data transfers in the monitored network (download and upload). These hosts cause the major utiliz...	•••
Hosts with Top Download Transfers in the Network	Monitoring Center	Custom	This chapter summarizes hosts with top download data transfers in the monitored network. These hosts cause the majo	•••
Hosts with Top Flows	Monitoring Center	Custom	This chapter summarizes network hosts with top number of flows in the monitored network. If there is an excessive num	•••
Hosts with Top Upload Transfers in the Network	Monitoring Center	Custom	This chapter summarizes network hosts with top upload data transfers in the monitored network. These hosts cause the major utilization of ...	•••

Configuration

Configuration is a page that lets you configure various settings in your Flowmon.

- Presets
- Topologies

Presets

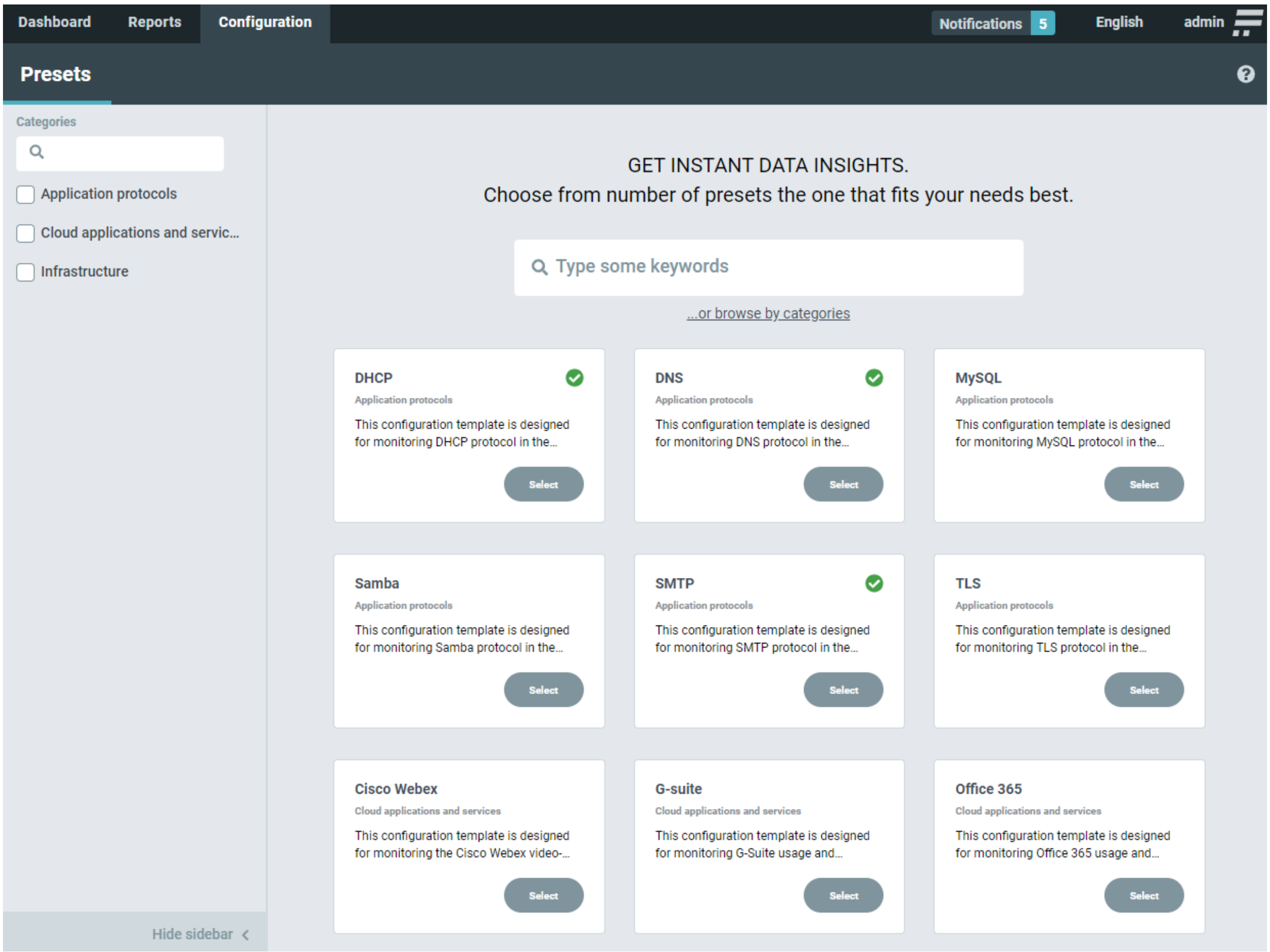
Presets provide a predefined configuration for specific use cases. You can pick a monitoring use case from the gallery. By applying the preset, all required configuration objects (profiles, channels, chapters, widgets, reports) are created.

The system checks the services portal for new or updated presets automatically every 12 hours. Click **Refresh** at the bottom of the page to refresh all presets available for this version.

Presets require the Flowmon appliance to have access to services.flowmon.com .

Presets Gallery

Presets gallery provides an overview of available presets. You can search through presets based on their name and description. Use the sidebar for quick filtering based on category. Click the preset card to see more details. Click **Select** to add the preset to the list. You can select and install multiple presets at a time.



GET INSTANT DATA INSIGHTS.
Choose from number of presets the one that fits your needs best.

DHCP ✓
Application protocols
This configuration template is designed for monitoring DHCP protocol in the...

DNS ✓
Application protocols
This configuration template is designed for monitoring DNS protocol in the...

MySQL
Application protocols
This configuration template is designed for monitoring MySQL protocol in the...

Samba
Application protocols
This configuration template is designed for monitoring Samba protocol in the...

SMTP ✓
Application protocols
This configuration template is designed for monitoring SMTP protocol in the...

TLS
Application protocols
This configuration template is designed for monitoring TLS protocol in the...

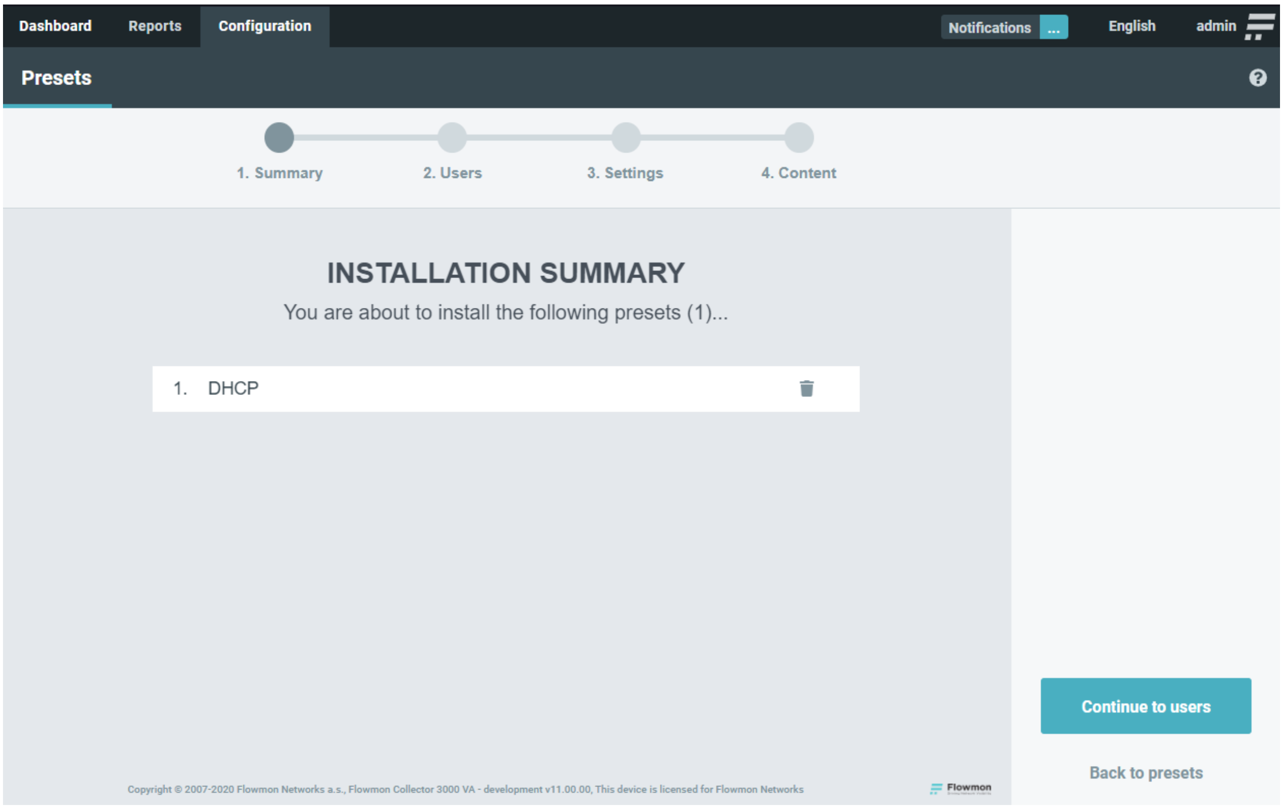
Cisco Webex
Cloud applications and services
This configuration template is designed for monitoring the Cisco Webex video-...

G-suite
Cloud applications and services
This configuration template is designed for monitoring G-Suite usage and...

Office 365
Cloud applications and services
This configuration template is designed for monitoring Office 365 usage and...

Installation

Click **Proceed to install** to open the installation wizard. First, an overview of selected presets is available. You can remove the selected presets from the list, if needed.

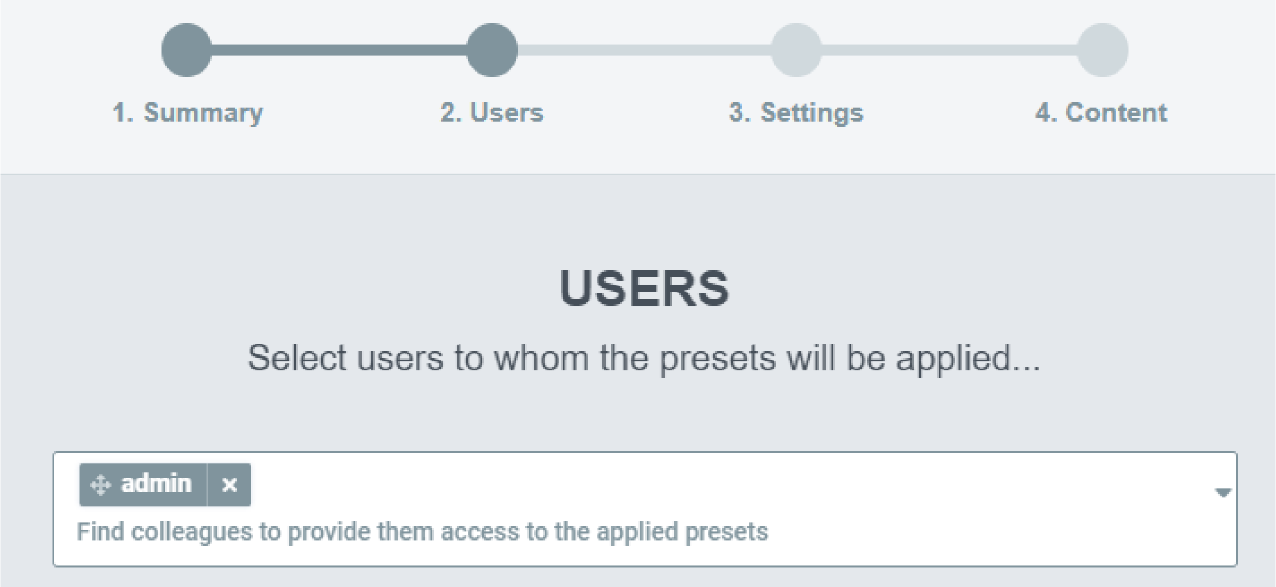


INSTALLATION SUMMARY
You are about to install the following presets (1)...

1. DHCP

Copyright © 2007-2020 Flowmon Networks a.s., Flowmon Collector 3000 VA - development v11.00.00, This device is licensed for Flowmon Networks

Second, select which users the preset will be applied to.



1. Summary 2. Users 3. Settings 4. Content

USERS

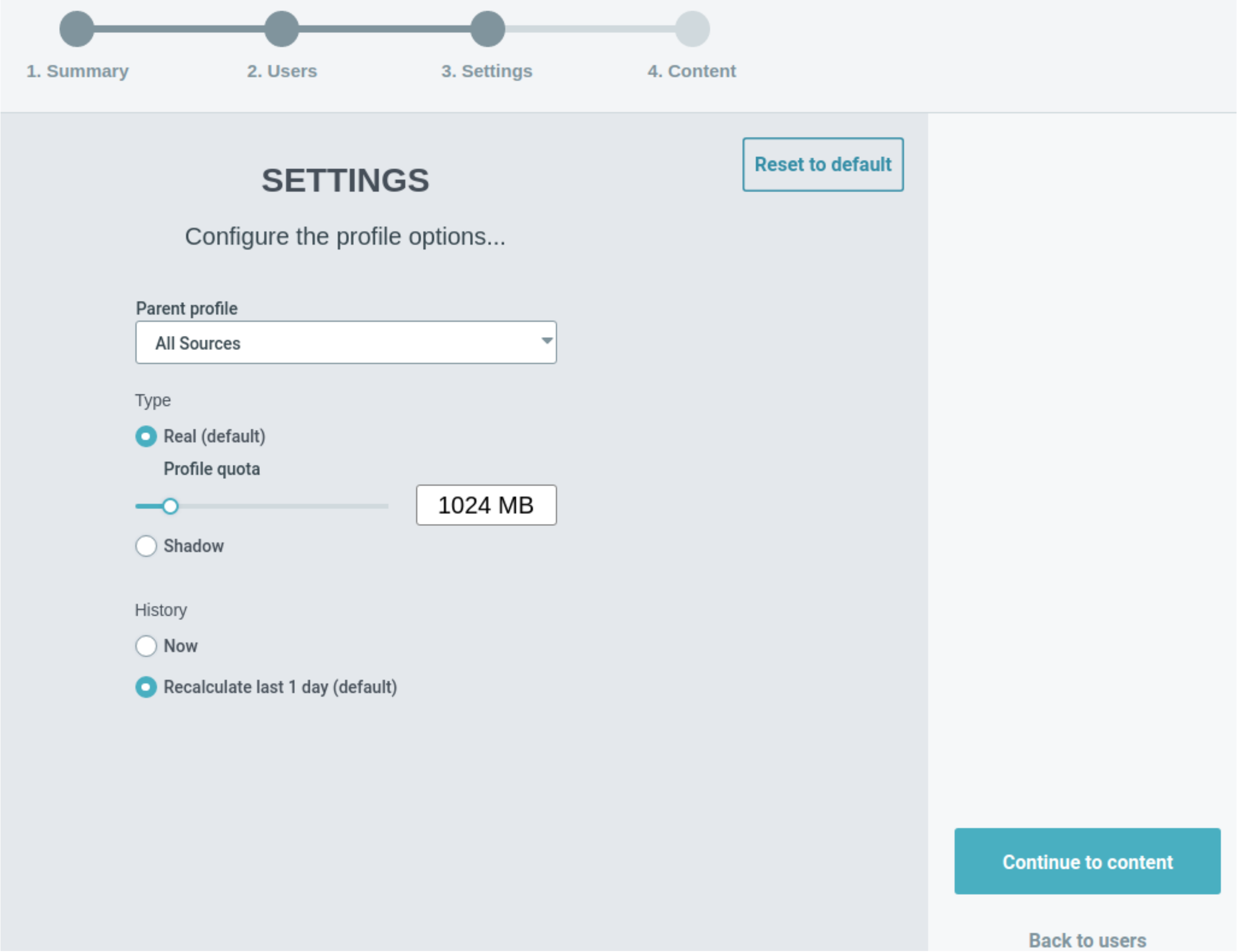
Select users to whom the presets will be applied...

admin ×

Find colleagues to provide them access to the applied presets

Next, you can modify the preset options:

- Parent profile – newly created profiles will use the selected profile as their parent
- Type – real or shadow (see 5.5.1 Profile types)
- Profile quota – set the maximum disk space that the newly created real profiles can use
- History – create profiles now or recalculate the data for the last day



1. Summary 2. Users 3. Settings 4. Content

SETTINGS

Reset to default

Configure the profile options...

Parent profile: All Sources

Type

● Real (default)

Profile quota: 1024 MB

○ Shadow

History

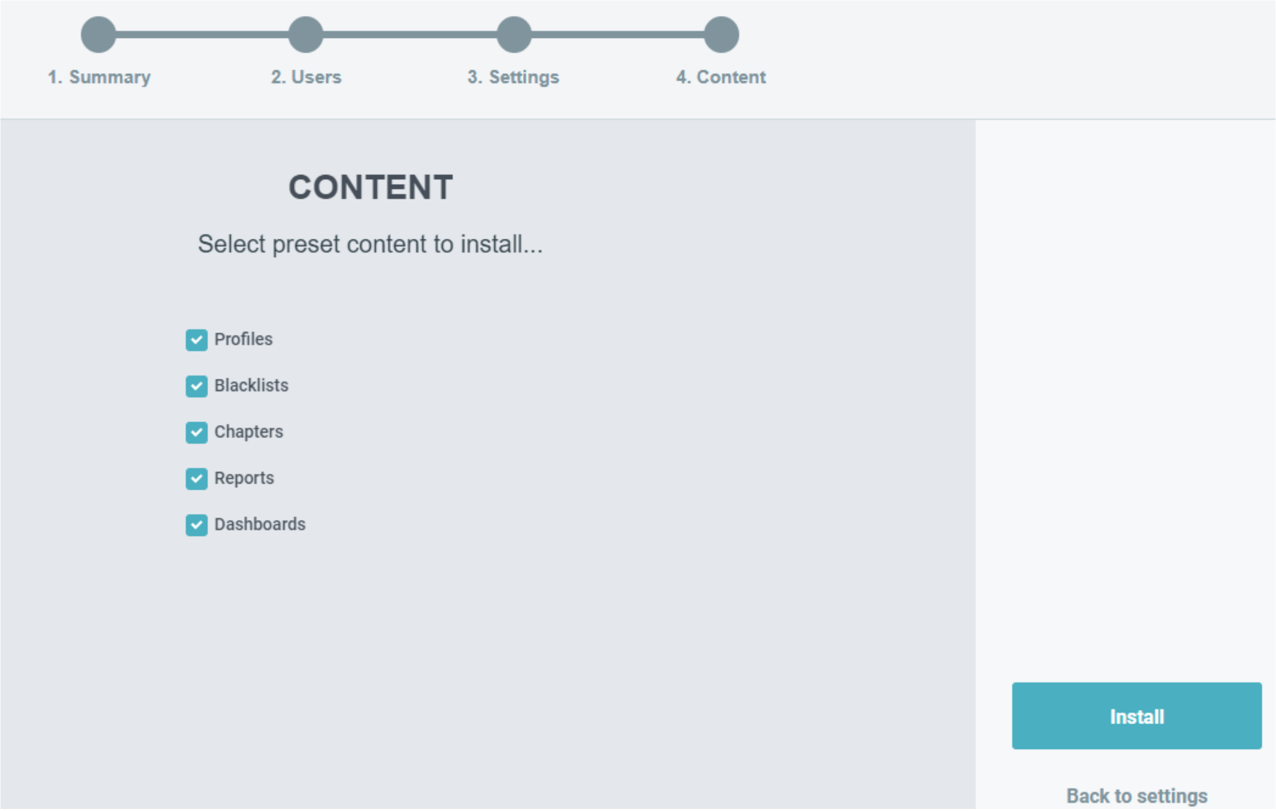
○ Now

● Recalculate last 1 day (default)

Continue to content

Back to users

Finally, choose what preset content to apply (Profiles, Blacklists, Chapters, Reports, or Dashboards). Some of the checkboxes are dependent on others – unchecking one can affect the others.

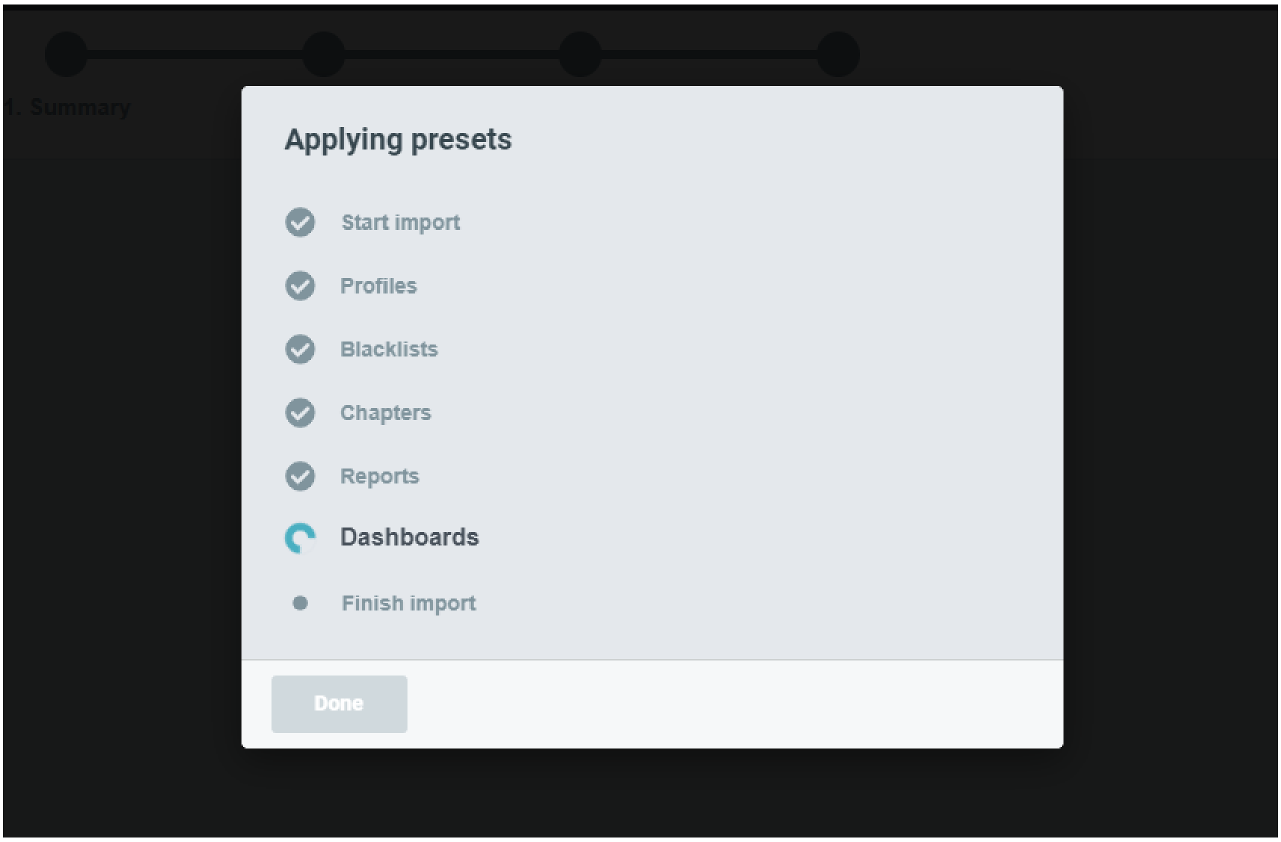


CONTENT

Select preset content to install...

☑ Profiles
☑ Blacklists
☑ Chapters
☑ Reports
☑ Dashboards

Click **Install** to run the installation. After the installation finishes, you will be redirected back to the Presets gallery.



Applying presets

✓ Start import
✓ Profiles
✓ Blacklists
✓ Chapters
✓ Reports
Dashboards
● Finish import

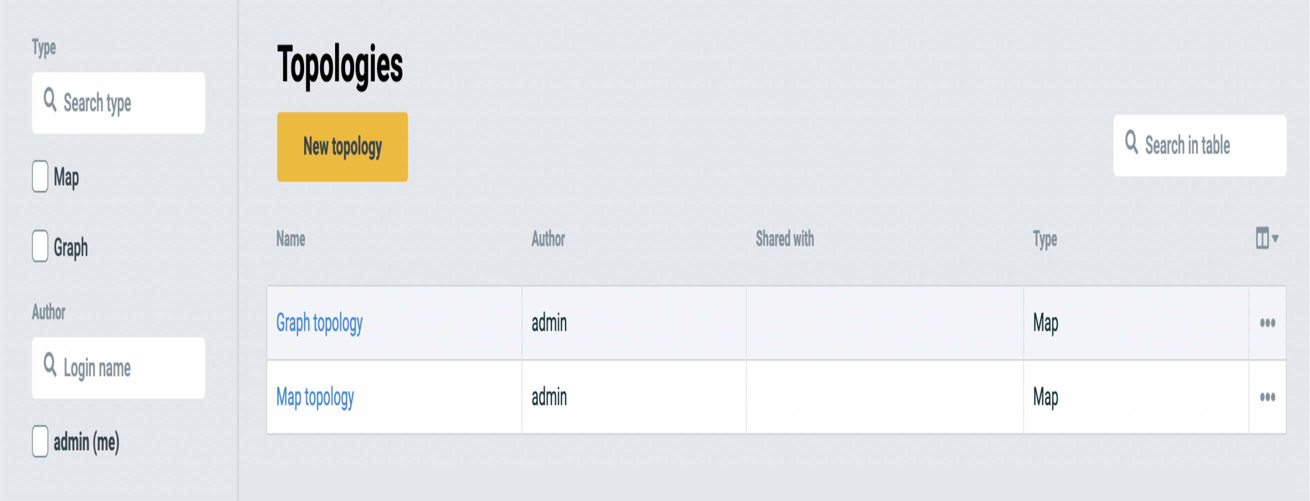
Topologies

Topologies allow users to draw a topology scheme of their network in a mode of map or a graph. Links can either be virtual or assigned to a specific channel. Assigned links visualize their utilization using a heatmap. Topology widgets can be used on a dashboard, so a user has an instant overview of the infrastructure (for more info, see the Widgets page). The link utilization is colored using a heatmap.

Topology configuration is managed in *Configuration > Topologies*. A list of existing topologies is available here and a user can edit an existing topology or create a new one. A user with the admin role is able to see topologies of all users.

Topologies overview page

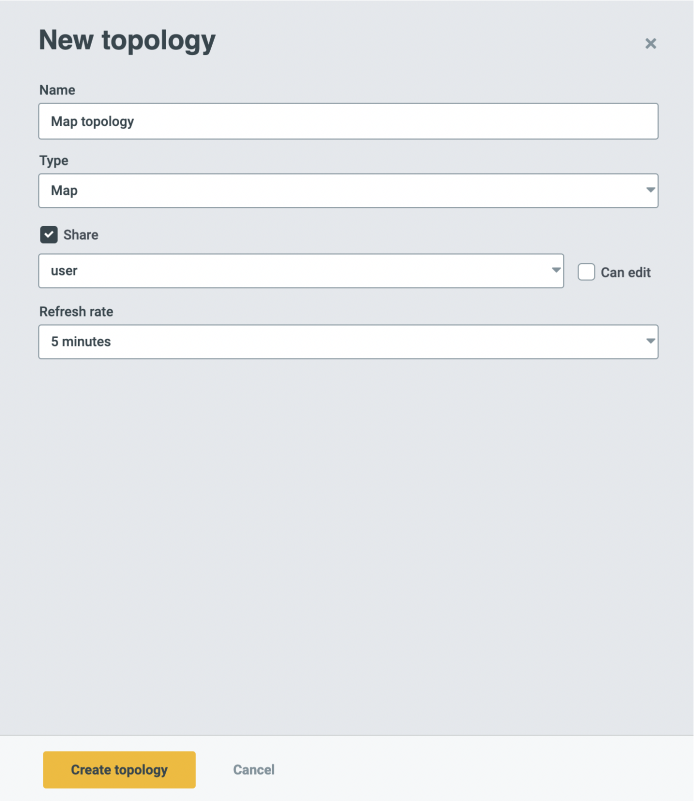
Topologies can be filtered using the left sidebar or the search function. User can **Edit** the topology name and properties or **Delete** the topology. By clicking the topology name, a user opens the **Topology detail** dialogue.



Name	Author	Shared with	Type	
Graph topology	admin		Map	•••
Map topology	admin		Map	•••

A new topology can be created by clicking the **New topology** button. The respective form includes

- **Name** of the topology.
- **Type** of the topology **-** user chooses between a graph type and a map type. The graph type provides a blank canvas to capture a logical topology while the map one places objects on a map. Please note that the type cannot be changed once the topology is created. To display a map topology, the client accessing the Flowmon web interface must be connected to the Internet.
- **Share** with user or role. The "Can edit" checkbox can be ticked to allow the users to perform changes in the topology.
- **Refresh rate** for **topology detail** page.



New topology

Name

Map topology

Type

Map

☑ Share

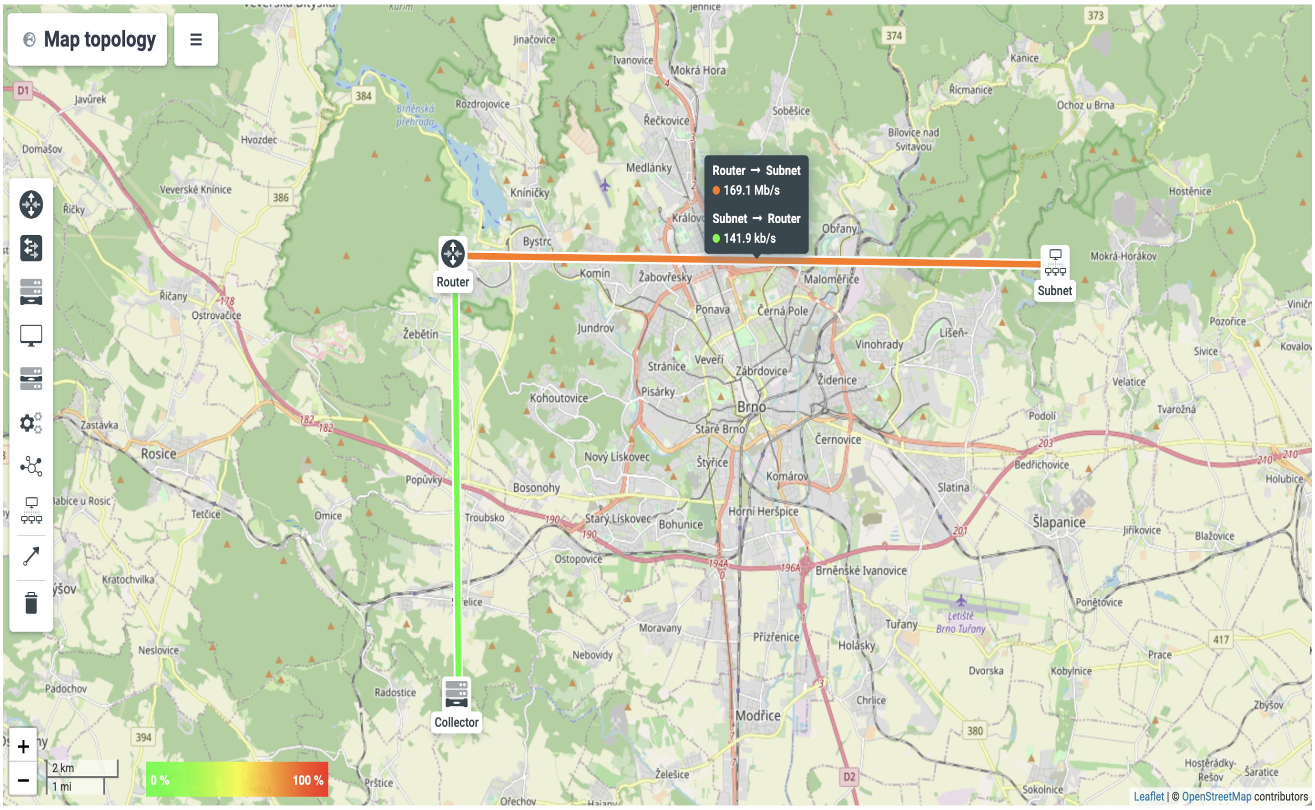
user ☐ Can edit

Refresh rate

5 minutes

Topology detail

After clicking on the name of the topology in the topologies list, user gets redirected to a topology detail page. Here, the user can edit the topology by adding, editing or removing nodes and links. Links are coloured based on how much of its bandwidth is being used. Information about the size of the traffic is available in a tooltip which appears when hovering over a link.

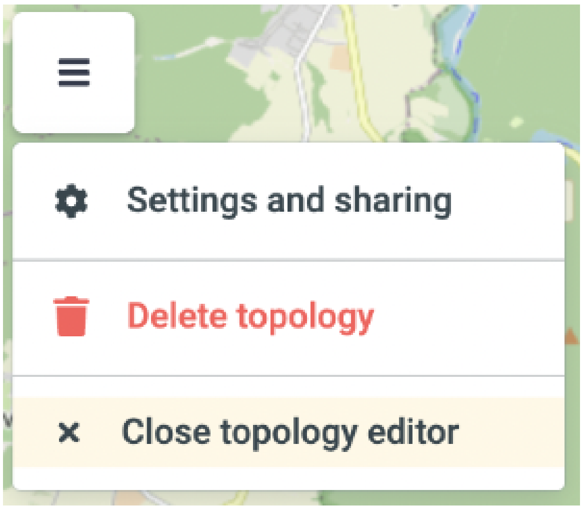


Router → Subnet
● 169.1 Mb/s

Subnet → Router
● 141.9 kb/s

Editing the topology

On top of the page next to the topology name there is a menu with options to edit topology settings, delete the topology or close the topology detail page and come back to list view of all topologies.

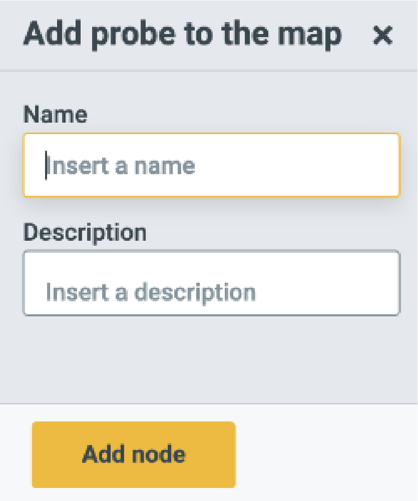


Editing topology content

On the left hand side, there is a control panel from which the user can choose elements to be added to the topology. First section contains various types of nodes, second section consist of an icon for adding a link and at the bottom of the control panel there is an icon used for deletion of elements already in the topology. The distinction between the node types only serves as a way to visually differentiate individual kinds of points in a topology and don't have any specific function in terms of the topology visualization itself.

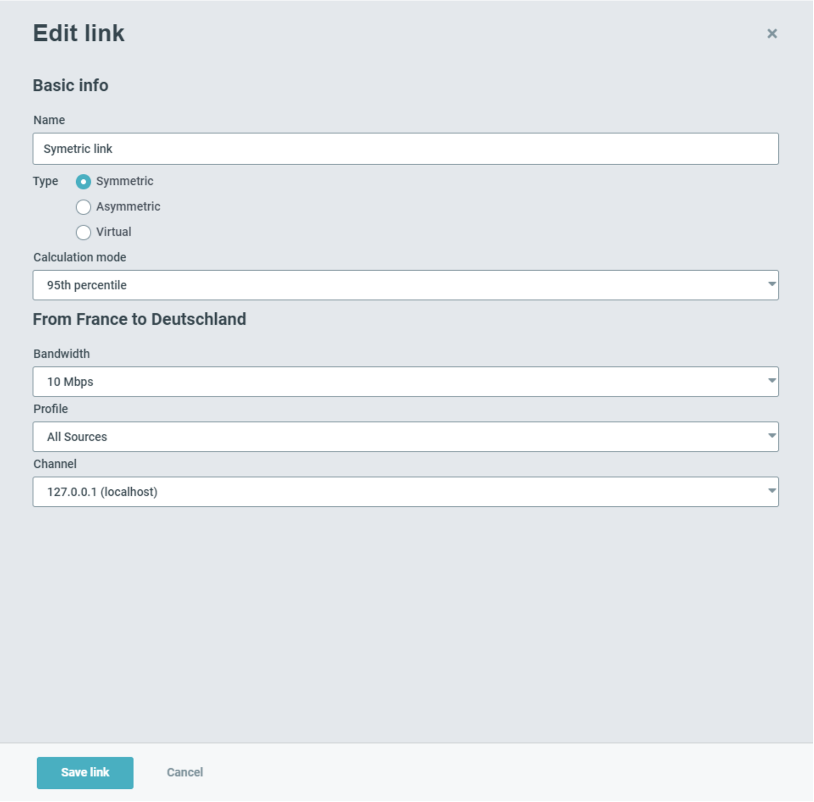
To add a new node or a link, the user clicks on an icon in the control panel and then clicks on a place on the map to place the node or clicks on two existing nodes to add a link between them. Location of nodes can be changed using a simple drag and drop and elements can be edited by clicking on them. To delete an element, select the icon of a trash can from the control panel and click on an element you wish to delete.

When adding a node, a name and a description can be set.



When adding a link, the user chooses from on of the three link types (described below), mode of calculation, bandwidth and a profile with a channel as the source of data.

- **Symmetric** - a bandwidth, profile and channel are set.
- **Asymmetric** - a pair of bandwidths, a profile and channel are set.
- **Virtual** - no bandwidth, profile or channel is assigned.



Edit link

×

Basic info

Name: Symetric link

Type: ● Symmetric ○ Asymmetric ○ Virtual

Calculation mode: 95th percentile

From France to Deutschland

Bandwidth: 10 Mbps

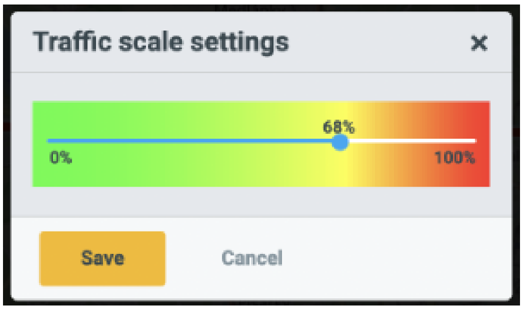
Profile: All Sources

Channel: 127.0.0.1 (localhost)

Edit link

Editing the traffic scale

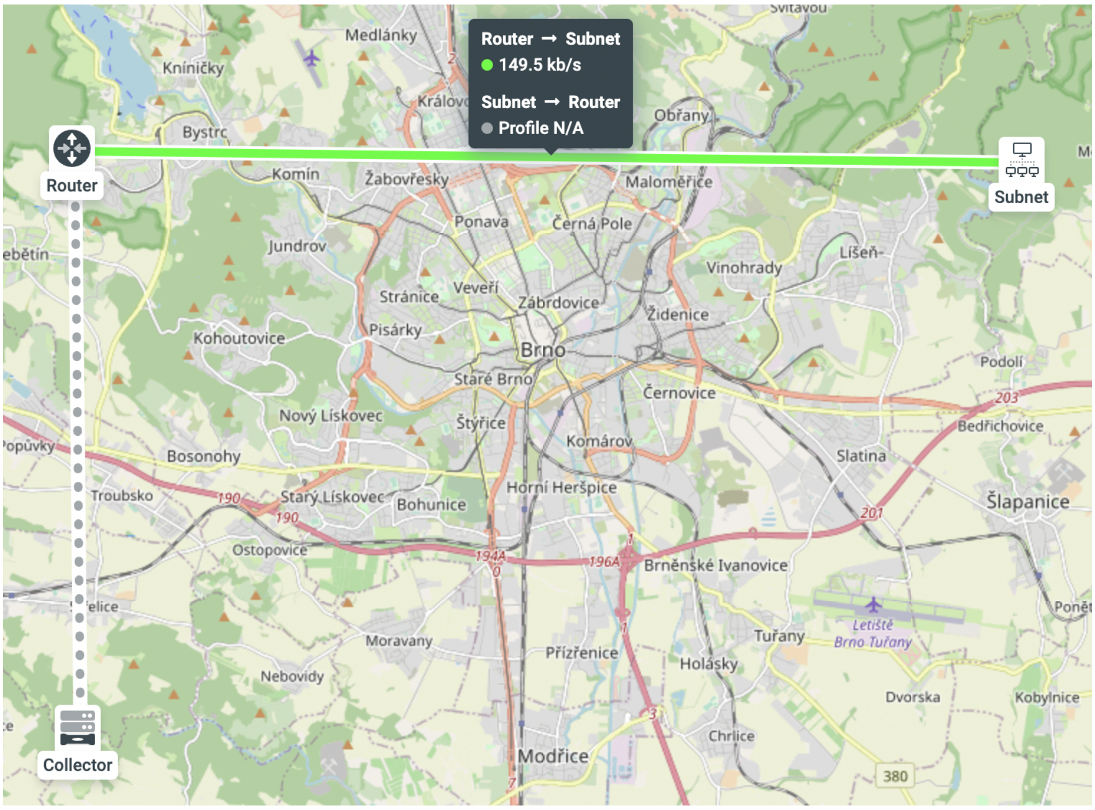
On the bottom left corner a traffic scale heat map controller is located. After clicking on it, the user can set the threshold at which topology links change colour from green to yellow or red signifying that current traffic in a link is a given percentage of the link's total bandwidth.



Traffic scale settings

Restricted access to topology content

If a user doesn't have access rights to a profile used in a topology link (e.g. in case when a topology was shared to a user by another user with more access rights), traffic summary for such links is not available in the topology detail. In case of a symmetric link or an asymmetric link with both profiles unavailable a dashed line is shown. For an asymmetric link with profile in one direction accessible by the current user, the link is colored and summary of traffic is available in a tooltip when hovering over with a mouse.



General

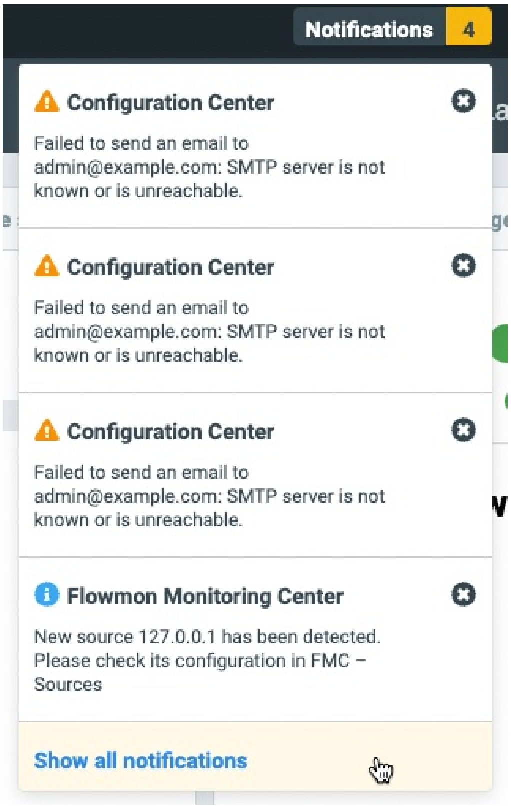
In this section, we describe other miscellaneous functionalities.

- [Notifications]
- [Table Functionalities]

Notifications

List of notifications

To see recent notifications, click on the Notifications button in the top right corner of the navigation bar and a pop up list appears. Click "Show all notifiactions" to go the the notifications page.



Configuration Center

Failed to send an email to admin@example.com: SMTP server is not known or is unreachable.

Configuration Center

Failed to send an email to admin@example.com: SMTP server is not known or is unreachable.

Configuration Center

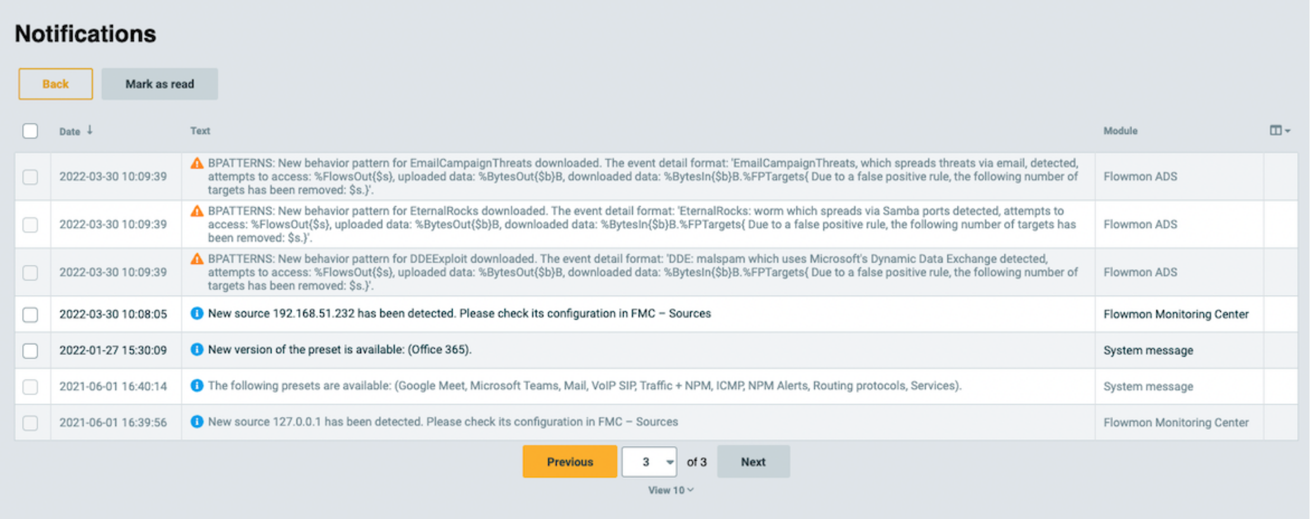
Failed to send an email to admin@example.com: SMTP server is not known or is unreachable.

Flowmon Monitoring Center

New source 127.0.0.1 has been detected. Please check its configuration in FMC – Sources

Notifications Page

On the notifications page, it is possible to see older notifications and also mark notifications as read.



Notifications

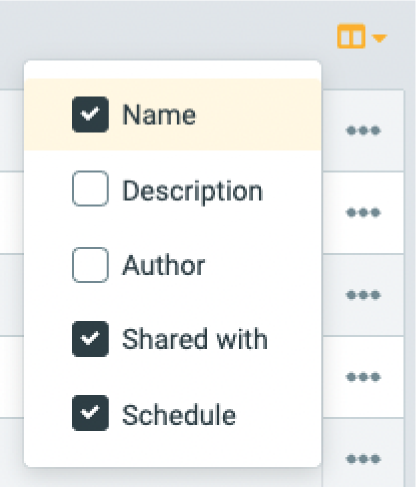
□	Date ↓	Text	Module
□	2022-03-30 10:09:39	BPATTERNS: New behavior pattern for EmailCampaignThreats downloaded. The event detail format: 'EmailCampaignThreats, which spreads threats via email, detected, attempts to access: %FlowsOut{$s}, uploaded data: %BytesOut{$b}B, downloaded data: %BytesIn{$b}B.%FPTargets{ Due to a false positive rule, the following number of targets has been removed: $s.}'.	Flowmon ADS
□	2022-03-30 10:09:39	BPATTERNS: New behavior pattern for EternalRocks downloaded. The event detail format: 'EternalRocks: worm which spreads via Samba ports detected, attempts to access: %FlowsOut{$s}, uploaded data: %BytesOut{$b}B, downloaded data: %BytesIn{$b}B.%FPTargets{ Due to a false positive rule, the following number of targets has been removed: $s.}'.	Flowmon ADS
□	2022-03-30 10:09:39	BPATTERNS: New behavior pattern for DDEExploit downloaded. The event detail format: 'DDE: malspam which uses Microsoft's Dynamic Data Exchange detected, attempts to access: %FlowsOut{$s}, uploaded data: %BytesOut{$b}B, downloaded data: %BytesIn{$b}B.%FPTargets{ Due to a false positive rule, the following number of targets has been removed: $s.}'.	Flowmon ADS
□	2022-03-30 10:08:05	New source 192.168.51.232 has been detected. Please check its configuration in FMC – Sources	Flowmon Monitoring Center
□	2022-01-27 15:30:09	New version of the preset is available: (Office 365).	System message
□	2021-06-01 16:40:14	The following presets are available: (Google Meet, Microsoft Teams, Mail, VoIP SIP, Traffic + NPM, ICMP, NPM Alerts, Routing protocols, Services).	System message
□	2021-06-01 16:39:56	New source 127.0.0.1 has been detected. Please check its configuration in FMC – Sources	Flowmon Monitoring Center

Table Functionalities

Throughout Dashboard and Reports you can find table views, which provide the user with certain functionalities. These may include **showing/hiding columns**, **sorting values**, **search**, **reordering columns** and **resizing columns**.

Showing and hiding columns

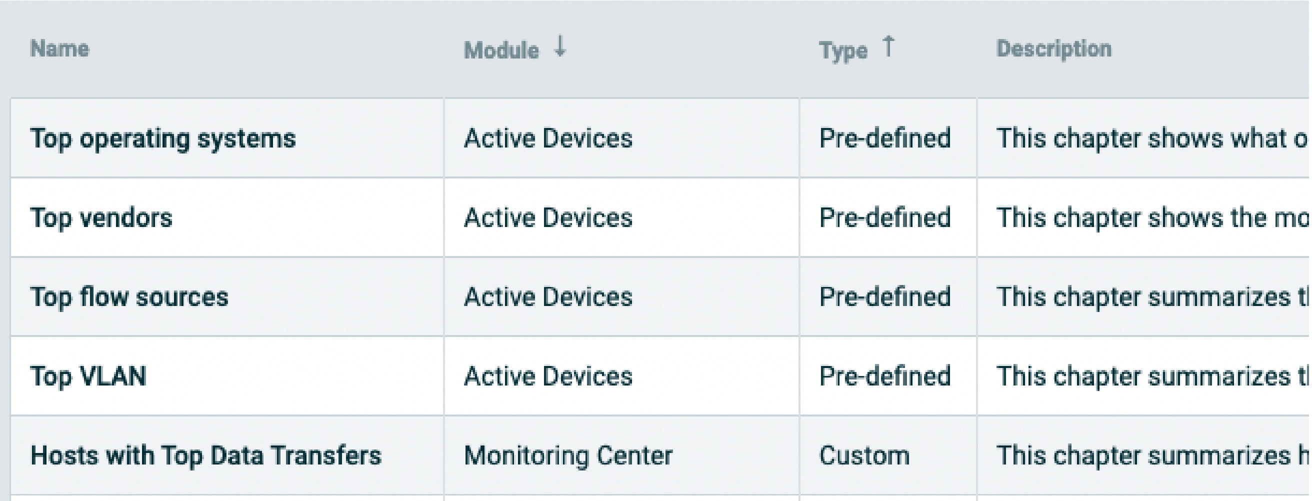
To select which columns should be visible, click on the icon in the top right corner of the table (e.g., in the reports list view).



☑ Name
□ Description
□ Author
☑ Shared with
☑ Schedule

Sorting values

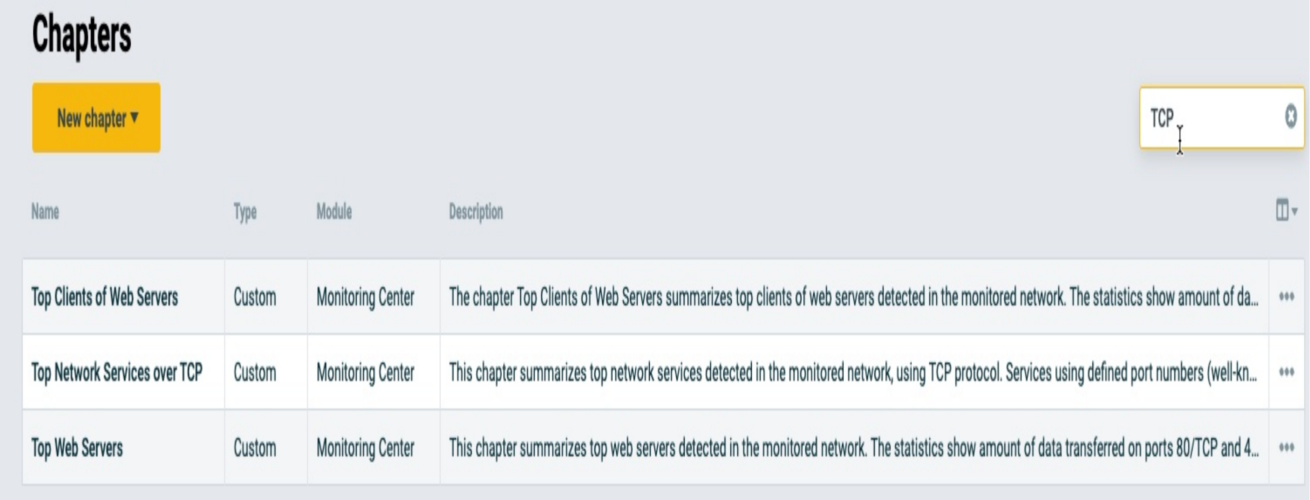
To sort the table according to values in a given column, click on the column header and an arrow appears signifying ascending or descending sorting. Use shift+click to sort by multiple columns.



Name	Module ↓	Type ↑	Description
Top operating systems	Active Devices	Pre-defined	This chapter shows what o
Top vendors	Active Devices	Pre-defined	This chapter shows the mo
Top flow sources	Active Devices	Pre-defined	This chapter summarizes t
Top VLAN	Active Devices	Pre-defined	This chapter summarizes t
Hosts with Top Data Transfers	Monitoring Center	Custom	This chapter summarizes h

Search

In the list view for reports, chapters, schedules or topologies, you can search entries with a word or phrase included in any of the columns.



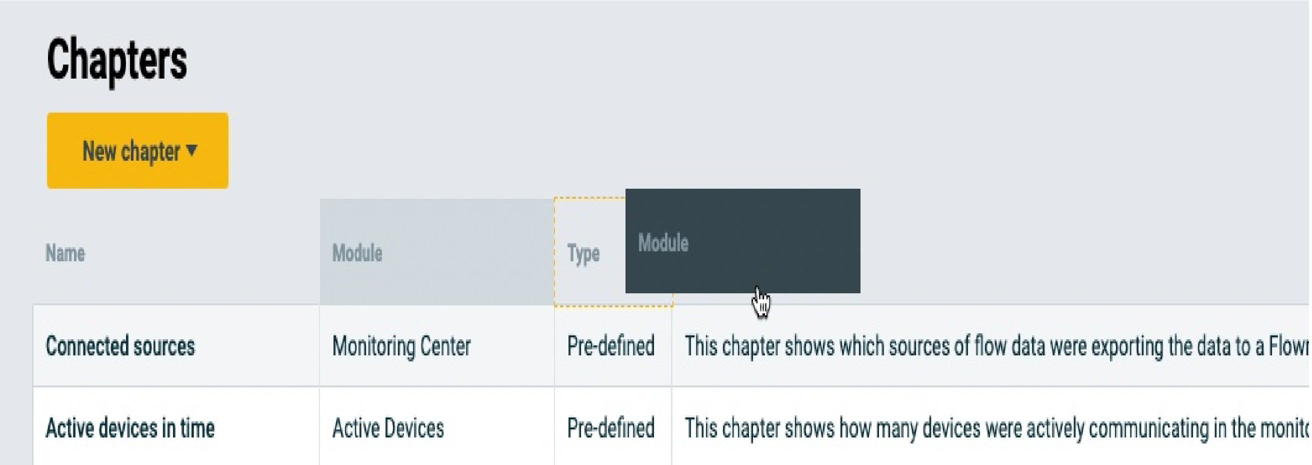
Chapters

TCP

Name	Type	Module	Description
Top Clients of Web Servers	Custom	Monitoring Center	The chapter Top Clients of Web Servers summarizes top clients of web servers detected in the monitored network. The statistics show amount of da...
Top Network Services over TCP	Custom	Monitoring Center	This chapter summarizes top network services detected in the monitored network, using TCP protocol. Services using defined port numbers (well-kn...
Top Web Servers	Custom	Monitoring Center	This chapter summarizes top web servers detected in the monitored network. The statistics show amount of data transferred on ports 80/TCP and 4...

Reordering columns

You can reorder columns using drag and drop.

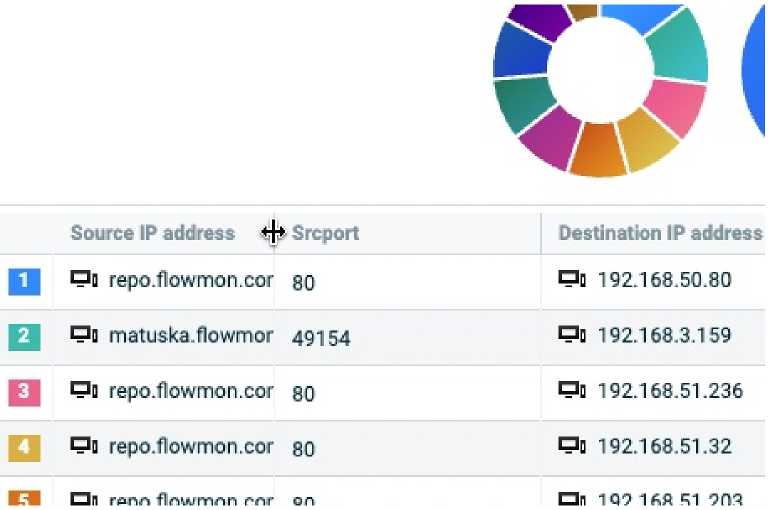


Chapters

Name	Module	Type	
Connected sources	Monitoring Center	Pre-defined	This chapter shows which sources of flow data were exporting the data to a Flow
Active devices in time	Active Devices	Pre-defined	This chapter shows how many devices were actively communicating in the monit

Resizing columns

Columns can be resized by dragging the edge of a column's header.



	Source IP address	Srcport	Destination IP address
1	repo.flowmon.cor	80	192.168.50.80
2	matuska.flowmor	49154	192.168.3.159
3	repo.flowmon.cor	80	192.168.51.236
4	repo.flowmon.cor	80	192.168.51.32
5	repo.flowmon.cor	80	192.168.51.203

Flowmon Modules

The functionality of Flowmon appliances can be extended by several modules for various tasks like Network behavioral analysis system (Flowmon ADS), DDoS attacks detection and mitigation (DDoS Defender), Application performance monitoring (Flowmon APM) and others (see Flowmon Networks website for more details).

The Flowmon device can be monitored via this systems using pre-installed agents. The configuration of these agents is performed under the user **flowmon** or using the sudo command.

SNMP Daemon

The Flowmon device is delivered with pre-installed SNMP daemon for easy remote device monitoring. The configuration file **snmpd.conf** is located in the **/etc/snmp** directory and can be modified by the **flowmon** user (locally or via ssh). To apply changes in this file run the following command:

```
 sudo /sbin/service snmpd restart
```

In case your modifications of snmpd.conf file could influence the clients connection (especially SNMP version and community string), you must modify the **/var/www/app/FccModule/models/Device.php** file too! You must modify the variables below. If you don't perform this modification, you won't be able to start/restart Flowmon monitoring port on the probe!

```
 // SNMP settings

public $prg_snmpwalk = "/usr/bin/snmpwalk";
public $snmp_version = "2c";
public $snmp_community = "public";
```

Zabbix Agent

The Flowmon device is delivered with pre-installed Zabbix agent. This module allows easy remote monitoring via centralized monitoring system (which can be installed on the Flowmon Collector or elsewhere).

Zabbix agent configuration file is located in **/etc/zabbix/zabbix_agentd.conf**. To apply the changes, please restart the agent as follows.

```
sudo /sbin/service zabbix-agent restart
```

Contact Flowmon

Contacts

Flowmon Networks a.s.

Škrobárenská 5

61700 Brno

Web: www.flowmon.com

Email: info@flowmon.com

Tel.: +420 530 510 600

Feedback

We would be pleased if you tell us your comments to this text (typing errors, incomplete or unclear information). Please, contact us via email support@flowmon.com.

Copyright