

What's new in Flowmon 8.02?

New version of our flag ship product has been released as a Flowmon 8.02. One of the most important feature is reliable and encrypted flow forwarding option. Flowmon 8.02 also brings reinvented view on Active Devices as well as new active device related widgets for Flowmon Dashboard. In addition, Flowmon 8.02 supports IPFIX items with variable length and Cisco AVC HTTP values.

At-a-glance insight

IPFIX via TCP connection

Encrypted flow forwarding

IPFIX items with variable length

Cisco AVC HTTP Support

New views on Active Devices

Strengthen security for Remote Access

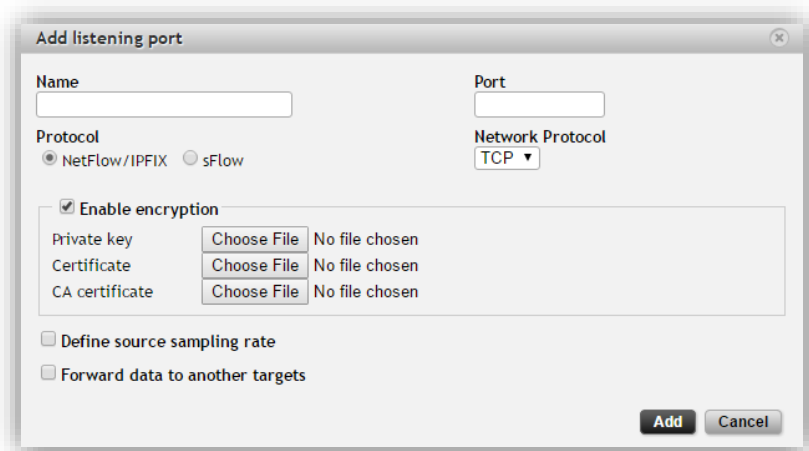
New customer stories

Check out our new [Success Stories](#) of customers relying on Flowmon.

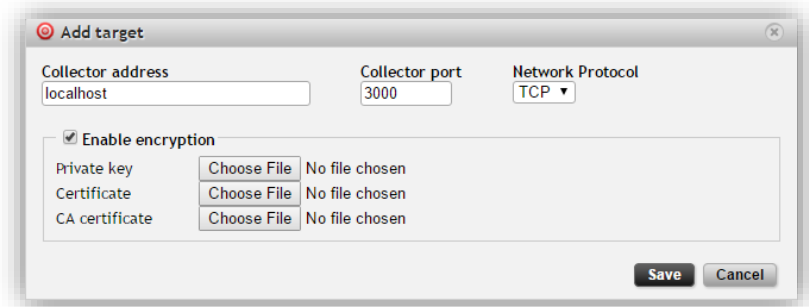


Reliable and secured IPFIX data transfer

Flowmon Collector traditionally used protocol UDP for receiving flow data. Since Flowmon 8.02, collector is able to receive IPFIX using TCP and TCP/TLS connection.



Received flow data can be forwarded encrypted to multiple different targets using TCP/TLS protocol. In this case, collector key and certificate together with CA certificate must be provided.



Thanks to these features, it is possible to provide reliable and encrypted communication between collectors.

IPFIX items with variable length and AVC HTTP Support

Flowmon 8.02 supports IPFIX items with variable length. Flowmon Collector can process Cisco AVC HTTP values (HTTP hostname and URL from Cisco devices). Cisco Application Visibility and Control (AVC) provides application-level classification, monitoring, and traffic control to reduce network operating costs. Another important benefits include faster troubleshooting, less network downtime and greater visibility of application usage and performance.

Strengthen security for Remote Access

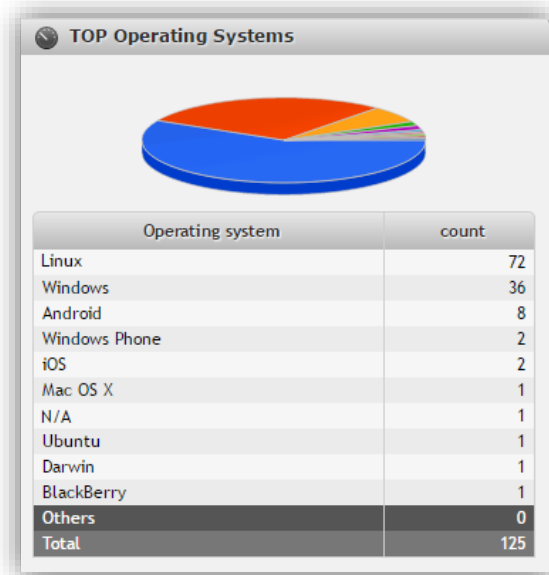
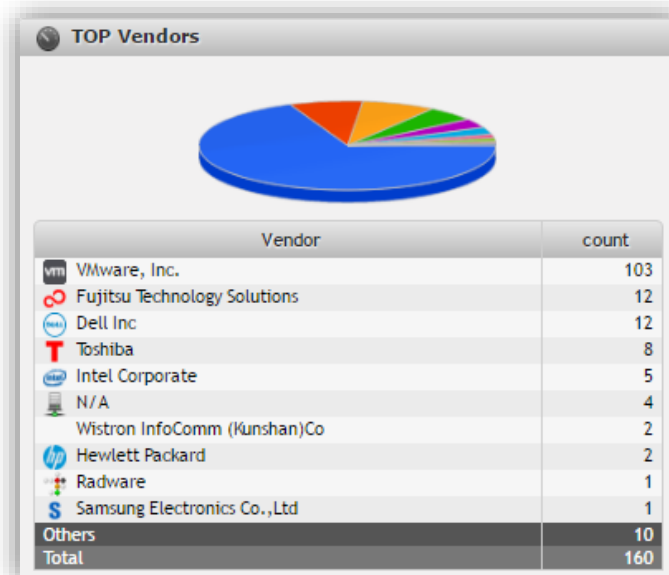
New security features are available in Flowmon Configuration Center. IP access restrictions can be defined for remote access. In default settings, there are no IP address restrictions (all IP addresses can access). Administrator can add IP addresses or subnets to limit access to provided addresses or ranges only.

In addition to IP restrictions, Flowmon’s integrated firewall is configured for both IPv4 and IPv6.

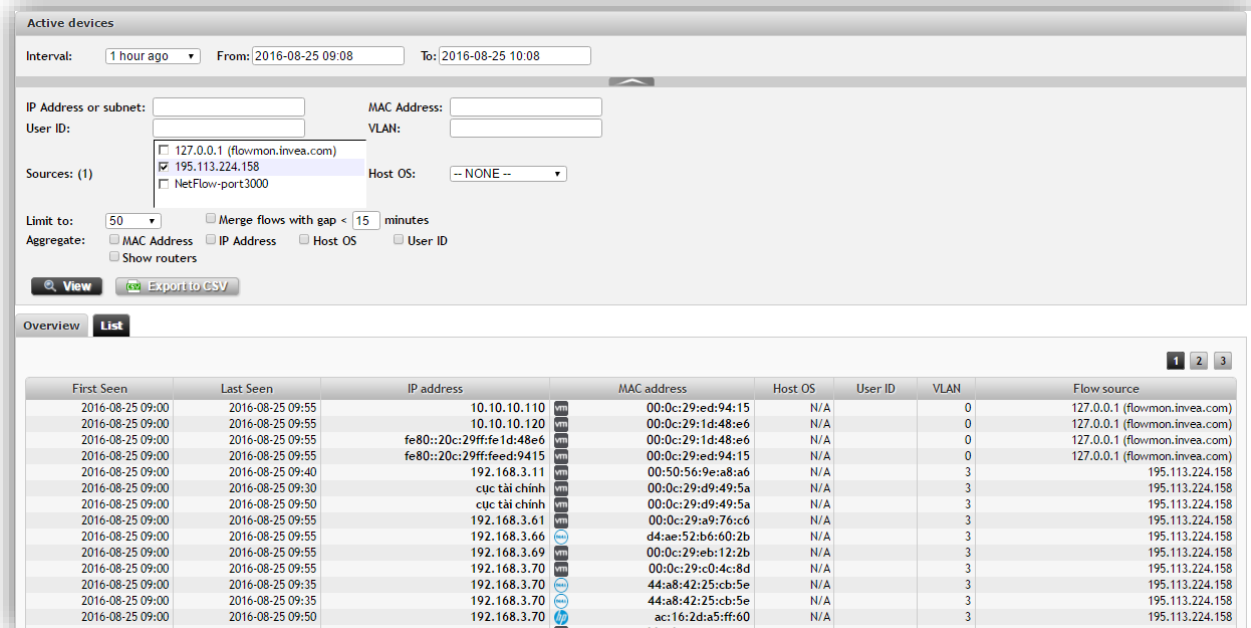


Active Devices

Flowmon 8.02 brings new views on Active devices. Section Active devices in FMC has a new Overview tab with dashboard lookup providing useful statistics. These statistics make it easier to see top flow sources, active devices in time, IP families, and other information related to active devices. Moreover, these new widgets can be added to central Flowmon Dashboard as well.



Active Devices offer flexible filtering options including aggregation.

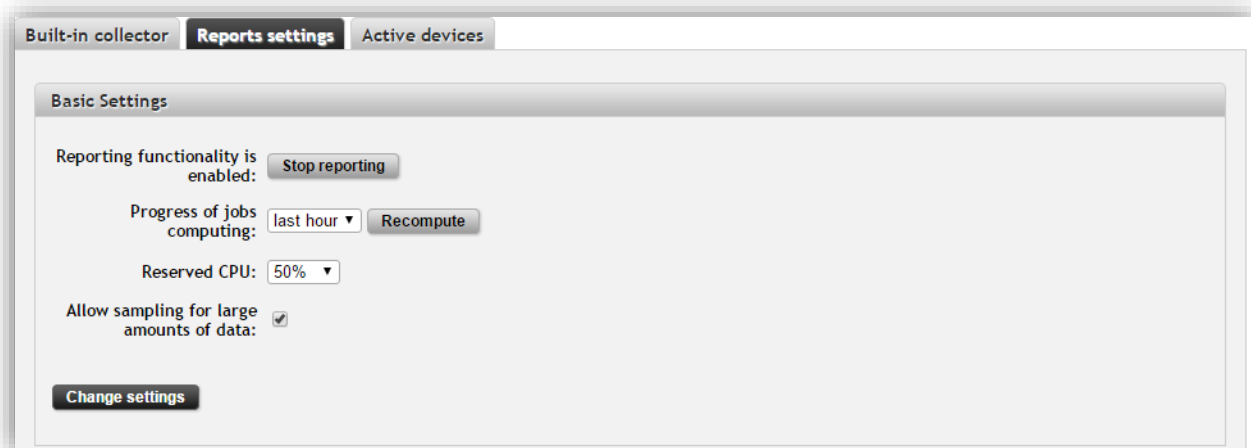


The screenshot shows the 'Active devices' configuration page. At the top, there are filters for 'Interval' (1 hour ago), 'From' (2016-08-25 09:08), and 'To' (2016-08-25 10:08). Below this are input fields for 'IP Address or subnet', 'MAC Address', 'User ID', and 'VLAN'. A 'Sources' list includes '127.0.0.1 (flowmon.invea.com)', '195.113.224.158' (checked), and 'NetFlow-port3000'. There are also options for 'Limit to' (50) and 'Merge flows with gap < 15 minutes'. The 'Aggregate' section has checkboxes for 'MAC Address', 'IP Address', 'Host OS', and 'User ID', with 'Show routers' also checked. A 'View' button and an 'Export to CSV' button are present.

Below the configuration area is a table with columns: First Seen, Last Seen, IP address, MAC address, Host OS, User ID, VLAN, and Flow source. The table contains 18 rows of data, including entries for IP addresses like 10.10.10.110, 10.10.10.120, and 192.168.3.11, and MAC addresses like 00:0c:29:ed:94:15 and 00:50:56:9e:a8:a6.

Sampling option in Report settings

To speed up reports computation over large amounts of data, sampling can be enabled in Reports settings (Flowmon Configuration Center). Sampling for report's computation does not affect the accuracy of data.



The screenshot shows the 'Reports settings' tab in the configuration center. Under 'Basic Settings', there is a 'Reporting functionality is enabled:' section with a 'Stop reporting' button. Below that is 'Progress of jobs computing:' with a 'last hour' dropdown and a 'Recompute' button. The 'Reserved CPU:' is set to '50%'. There is a checkbox for 'Allow sampling for large amounts of data:' which is checked. A 'Change settings' button is at the bottom.

SNMP trap alert with alert details

Alerts allow to trigger combination of specific actions such as sending of an email, executing user defined script, posting a syslog message or SNMP trap. The SNMP trap now contains alert details in the trap, to provide accurate information for administrator.

Sources

IP address for SNMP connection can be modified per flow source. It allows us to adjust the IP address for reading SNMP information for each source.