Plixer Documentation

Release 1.0.2

Plixer

Oct 31, 2023

PLIXER ONLINE DOCUMENTATION

The Plixer Online Documentation library houses all Plixer product documentation, including implementation guides, configuration instructions, and additional references.

For further assistance, contact Plixer Technical Support.

CHAPTER

ONE

INTEGRATED SOLUTIONS

CHAPTER

TWO

PRODUCTS

CHAPTER

THREE

PLIXER TECHNICAL SUPPORT

Plixer Technical Support is available with an active maintenance contract. Contact our support team at:

- +1 (207) 324-8805 ext 4
- https://www.plixer.com/support/

3.1 Welcome

The Plixer Online Documentation library houses all Plixer product documentation, including implementation guides, configuration instructions, and additional references.

For further assistance, contact Plixer Technical Support.

3.1.1 Integrated Solutions

3.1.2 Products

3.1.3 Plixer Technical Support

Plixer Technical Support is available with an active maintenance contract. Contact our support team at:

- +1 (207) 324-8805 ext 4
- https://www.plixer.com/support/

3.2 Integrated Solutions

Harness the power of netflow and tap into your existing IT infrastructure to elevate network performance with the Plixer One Platform. Powered by Scrutinizer, our cost-effective integrated NPMD and NDR solutions deliver robust network and security intelligence to maximize your network security and efficiency with speed and scale.

3.2.1 Platform components

The features and functionality of Plixer Enterprise and Plixer Core are explained in greater detail in the following Plixer product manuals:

3.3 Product Lifecycle and End of Life Policy

Plixer is committed to providing customers with market leading products and solutions. Periodically, as part of the product lifecycle, it becomes necessary to discontinue older products, for technology and/or business reasons.

It is Plixer's goal to make this product lifecycle process as transparent as possible to our customers and partners, thereby enabling them to plan for upgrades, migrations, and purchases associated with their Plixer environment.

3.3.1 EOL products

The Plixer product matrix below shows products have been superceded and are no longer available. Please refer to Plixer's Product Release Policy document (below) to view more information on milestone definitions and timelines.

Product	Version	End of Sale date	End of Support date	Successor
Scrutinizer MDX product family (MDX-xxx)	All versions	December 31, 2019	March 31, 2023	Migrate to comparable SSRV or SCR product
Plixer Scrutinizer (SSRV and SCR)	Versions earlier than 18.20	August 31, 2020	August 31, 2021	Upgrade to supported release
Plixer Scrutinizer (hardware appliance)	Deployed on Dell PowerEdge system earlier than R740	November 30, 2019	End of current support term, or 5 years from original purchase (whichever occurs earlier)	Upgrade to supported hardware
Plixer Replicator	Version earlier than 18.14	August 31, 2020	August 31, 2021	Upgrade to supported release
Plixer FlowPro (all variants)	Version earlier than 18.12	August 31, 2020	August 31, 2021	Upgrade to supported release
Plixer Beacon (formerly Great Bay Software)	Version 6.2.0_24	Previously announced	November 30, 2021	Upgrade to supported release
Plixer Beacon	Version 6.1 (versions earlier than 6.1 have already reached end of Support previously)	Previously announced	March 18, 2020	Upgrade to supported release
Plixer Beacon	Gen3 appliance	May 31, 2017	May 31, 2022	Upgrade to supported hardware
Plixer Beacon	Gen2 appliance	April 30, 2014	April 3, 2019	Upgrade to supported hardware
Plixer Beacon	Gen1 appliance	February 1, 2010	July 1, 2015	Upgrade to supported hardware
Denika, Logalot, Mailinizer, OStivity, WebNM, WebTTS	All versions	All are beyond End of Sale	All are beyond End of Sale	N/A
Plixer Scrutinizer (free edition)	All versions	n/a	December 31, 2021	Paid version of product
Hardware appliances (1.8TB, 3.6TB, and 7.2TB)	All	12/31/2021	End of customer's current support agreement	Migration to new generation of appliance hardware
Plixer Risk Intelligence Module	All	12/31/2021	End of customer's current support agreement	Migration to new technology TBA
Plixer Scrutinizer (and corresponding PSI and PNI add-on modules)	Version 19.0	n/a	12/31/2022	Upgrade to supported release
Plixer Scrutinizer (and corresponding PSI and PNI add-on modules)	Version 19.1.x	n/a	09/30/2023	Upgrade to supported release

Note: Due to differences in release policies with acquired companies (such as Great Bay Software), the product schedules listed in the table above may deviate from the policy outlined in this document. Where differences occur, the table above takes precedence.

3.3.2 Product Release Policy

The following topics outline the intended release and lifecycle support plans for products and versions. The policy is intended to provide information required to plan for product upgrades and migration to replacement technologies.

Note: These topics covers product releases; product licensing - covering usage of the product – is handled under the terms specified in the EULA (End User Licensing Agreement). Product Support is covered under a separate policy.

3.3.2.1 Software Release Definitions

- **Major (Main) Release**: Major releases encompass new products, major architecture changes, major user interface (UI) changes, significant new features or capabilities/functionality additions, new solutions, and substantial innovation. Plixer's goal is for one Major product release per year.
- **Minor Release**: Minor releases include updates or enhancements/features to existing products, moderate administration or UI changes, and major bug fixes. Plixer's goal is for one Minor product release per year.
- **Patch Release:** A patch release incorporates bug fixes and security fixes. Patch releases will be incorporated into the next **Major** or **Minor** software release (whichever occurs first). Plixer's goal is to provide patch releases as needed, not to defined release schedule. (Note: earlier terminology may use the term 'Service Pack' when referring to a Patch Release.)

Note: Engineering Hotfixes, developed to resolve customer-specific support cases of high severity, are made broadly available to other customers in the next available release (**Major**, **Minor** or **Patch** release).

- **Content Update Release:** Plixer may release updated content – new reports, new or updated algorithms, etc – periodically, outside of a **Major** or **Minor** software release. Content Updates do not include new features and may be applied electively at the customer's discretion to any supported product release. Content updates will be incorporated into the next **Major** or **Minor** software release, whichever happens first.
- The software product version numbering scheme is defined as follows:

  (Major). (Minor). (Patch)

  Example: 18.16.02

where Major release is 18, Minor release is 16, Patch release is 2.

- The Content Update numbering scheme is defined as follows.

  CU.(YYMMDD)

  Example: CU.200310

where YYMMDD is the release year, month and day of the content update.

3.3.2.2 Supported Product Releases and Product Release End of Life Policy

Generally speaking, Plixer supports the most current product release and the release prior to that (in other words, we support two product releases).

Plixer will make commercially reasonable efforts to adhere to the following guidelines:

- The End of Life Period for a major software release "N" starts when the N+2 major release becomes Generally Available. For example, major product release 18.x begins EOL when major product release 20.x is made available. Customers running major release 18 should upgrade to major release 19 or major release 20.

Note: When major versions are released, only the last minor release on the "N" major release will be supported. In the example above, major release 18.x enters EOL and customers should be up-to-date on the last minor release for major release 18 for software support during the EOL support period.

- Likewise, the End of Life Period for a minor software release starts when the N+2 minor release becomes Generally Available. For example, product release 18.15 begins EOL when release 18.17 is made available. Customers running minor release 18.15 should upgrade to release 18.16 or 18.17.
- Plixer will support all GA software releases for a minimum of 12 months from their initial release date. The maximum total support life of a software product release is the lesser of three (3) years or the release of the N+2 version, inclusive of the General Availability period and software support period following the End of Life announcement.
- For all Cloud Services, only the current product release will be supported.

3.3.2.3 End of Life Software Support Policy

To ensure delivery of innovative and cost-effective products, Plixer may periodically discontinue specific products or versions of products and cloud services. At Plixer's sole discretion, such products or services may be discontinued regardless of the delivery method, including on-premises software, hardware and cloud services.

This policy applies to all Plixer Software product offerings that enter the End of Life process as of the Effective Date of this EOL Policy. For clarity, this applies to any Software that is included with Plixer Hardware or Appliances.

When commercially reasonable, Plixer will provide three (3) months' notice of an affected product's End of Sale (EOS), i.e., the last day the product can be ordered. Once the End of Sale date is reached, the affected product is no longer available for sale.

Plixer will make commercially reasonable efforts to provide Software Support for a maximum of 1 year after the effective End of Sale Date, unless otherwise specified. Plixer will not provide Software Support past the specified EOL date.

The list of EOS/EOL products is maintained on the Plixer website.

3.3.2.4 End of Life Hardware Support and Software/Hardware Support Bundles Policy

This policy applies to the physical components of Plixer's Hardware, Appliances or Software/Hardware Bundles (collectively referred to as Hardware). It covers EOL for various 'generations' of hardware platforms broadly shipped to customers.

- Plixer will exercise commercially reasonable efforts to provide 3 months notification prior to the effective End of Sale Date.
- Plixer will make commercially reasonable effort to provide Hardware Support for 3 years after the End of Sale Date. Provision of Hardware Support is subject to the terms of the support contract.

- Hardware Support contracts cannot extend past the published End of Support Date.

If the latest release of supported software requires a new hardware platform, or the customer's existing hardware has reached End of Support, the customer may be given an opportunity to purchase a comparable platform. In no case will a hardware product be provided at no cost if newer versions of the software will not run on the older hardware.

3.3.2.5 Definitions

General Availability – Product is generally available for Sale and Support on current Plixer Pricelist.

End of Life (EOL) Period - Refers to the timeframe beginning with the day Plixer announces a product is no longer available for purchase from the current Plixer Pricelist until the last date the product is formally supported by Plixer. If software version only, EOL Period refers to the timeframe beginning with the day Plixer announces a software version will no longer be available until it is no longer supported.

End of Sale Notification– This notification establishes when the discontinued product or software version will no longer be Generally Available. The End of Sale Notification begins the EOL period. This notification may be given by any means including, but not limited to, posting the EOS (End of Sale) notice on the Company's Website.

End of Sale Date– The date a product is no longer Generally Available for purchase.

End of Life Date – The last day that the product and/or software version is supported per the terms of the standard Software and Hardware Support offerings.

Cloud Services - means services offered on servers that are owned or managed by Plixer and provided to Customer as specified by the relevant Customer agreement. Access to the Cloud Services requires either an active support agreement or an active subscription, as required by the specific offering.

Content Updates – Include enhanced product components, such as new reports and new algorithms.

Software Support - Software Support includes available maintenance and technical support. Security updates and maintenance will continue until the end of the Software Support period.

Hardware Support - Hardware Support includes hardware warranty, new software/firmware versions, escalations, patches and maintenance releases, product updates, content updates, and available maintenance and technical support.

Software - means each Plixer software program that is (a) licensed from Plixer (and acquired during the Term from Plixer or an Authorized Reseller), and identified in the applicable agreement, or (b) embedded in or pre-loaded on Hardware acquired during the Term, but not identified in an agreement (which embedded or pre-loaded software is hereby deemed licensed from Plixer), in each case including Updates and Upgrades that Customer installs during any applicable Support period.

Hardware - means the Plixer or Plixer branded hardware equipment (together with all parts, elements, or accessories, and any combination of them) purchased during the Term from Plixer or an Authorized Reseller and identified in an applicable agreement, excluding any software or other intangible items (whether or not pre-loaded on hardware or subsequently loaded on hardware by Customer, Plixer, or any other person or entity).

Plixer and the Plixer logo are trademarks or registered trademarks of Plixer LLC.

3.4 Exporter Configuration

This page provides commonly requested flow and metadata configuration details, as requested by our customers.

3.4.1 NetFlow Configurations

3.4.1.1 AdTran NetVanta Router

The Adtran NetVanta Router supports NetFlow v9. For more information, please refer to the Adtran Web Site.

Only enable egress flows (i.e. no ingress) on Adtran routers. More information can be found on page 27 of the Adtran Configuration Guide.

3.4.1.2 APCON Appliance

How to configure an APCON appliance

3.4.1.3 Aruba Appliance

How to configure an Aruba appliance

3.4.1.4 Big Switch

How to configure a Big Switch

3.4.1.5 Blue Coat MACH5

How to configure a Blue Coat MACH5

3.4.1.6 Check Point Appliance

Check Point GAiA NetFlow Configuration

3.4.1.7 Check Point Firewall

NetFlow from a Check Point Firewall

3.4.1.8 Cisco 4605 series with a daughter card configured with VLANs

Bandwidth needs to be set explicitly at the VLAN:

```
ip route-cache flow infer-fields
ip flow ingress infer-fields
```

3.4.1.9 Cisco 7600 router

If you plan to export NetFlow statistics, globally enable NDE on the router by issuing the following commands:

```
configure terminal
ip flow-export destination
ip flow-export version
mls nde sender version
```

Enable NetFlow on individual interfaces by issuing the following commands:

```
configure terminal
interface
ip flow ingress
```

1. (Optional) To configure NetFlow sampling, do the following:
    1. Enable sampled NetFlow globally on the router (**mls sampling**).
    2. Enable sampled NetFlow on individual interfaces (**mls netflow sampling**).
2. Verify the NDE configuration to ensure that it does not conflict with other features such as QoS or multicast. Use the show ip interface command to verify the configuration.

These and other related commands can be found in the Cisco 7600 Series Cisco IOS Software Configuration Guide.

3.4.1.10 Cisco ACI

Cisco ACI NetFlow Support

3.4.1.11 Cisco APIC

Cisco APIC NetFlow Support

3.4.1.12 Cisco ASA FireSIGHT

Cisco ASA FireSIGHT Integration

3.4.1.13 Cisco ASA Firewall

How to enable NetFlow on your Cisco ASA gear

3.4.1.14 Cisco ASA Firewall (using ASDM)

Cisco ASA NetFlow Configuration Using ASDM

3.4.1.15 Cisco ASR 1000

Cisco High Speed Logging

3.4.1.16 Cisco ASR 9000

How to configure NetFlow on the Cisco ASR

3.4.1.17 Cisco Catalyst 2960-X

How to configure a Cisco 2960-X

3.4.1.18 Cisco Catalyst 3750 with a 3KX module

Cisco 3750-X NetFlow Support

3.4.1.19 Cisco Catalyst 3850

Cisco Flexible NetFlow Configuration Guide

3.4.1.20 Cisco Catalyst 4500

Catalyst 4500 Series Switch NetFlow Configuration Examples

3.4.1.21 Cisco Catalyst 4510 Switch IOS XE 3.6

Configuring a Cisco Catalyst 4510 Switch IOS XE 3.6

3.4.1.22 Cisco Catalyst 4948E switch

Exporting NetFlow-Lite from the Cisco 4948E switch

3.4.1.23 Cisco Catalyst (4000 Series running in Hybrid or Native Mode)

Configure the switch the same as an IOS device, but instead of the command

```
ip route-cache flow
```

Use the following command:

```
ip route-cache flow infer-fields
```

This series requires a Supervisor Engine IV with a NetFlow Services daughter card to support NDE.

3.4.1.24 Cisco Catalyst Switch (non-4000 Series)

Are you running CatOS? **Yes**

Router side:

Enter the following global commands.

```
ip flow-export source
ip flow-export version 5
ip flow-export destination
ip flow-cache timeout active
```

Enter the following command on each physical interface. You will need to log into each interface one at a time.

```
ip route-cache flow
```

Switch side:

```
set mls nde
set mls nde version 5
set mls flow full
set mls agingtime long 128
set mls agingtime 64
set mls bridged-flow-statistics enable
set mls nde enable
```

No

Enter the following global commands (all commands are entered in the router config -t option).

```
ip flow-export source
ip flow-export version 5
ip flow-export destination
ip flow-cache timeout active 1
mls nde sender version 5
mls flow ip interface-full
mls nde interface
mls aging long 64
mls aging normal 64
```

Enter the following command on each physical interface. You will need to log into each interface one at a time.

```
ip route-cache flow
```

3.4.1.25 Cisco Catalyst 6500/6000 Series Switch

Catalyst 6500/6000 Switches NetFlow Configuration and Troubleshooting

Configuring NetFlow on the MSFC guide.

3.4.1.26 Cisco Catalyst 6509 Switch

Cisco Catalyst 6509 NetFlow Support

3.4.1.27 Cisco Catalyst 9300 Switch

Cisco Catalyst 9300 NetFlow Support

3.4.1.28 Cisco IWAN

Cisco IWAN Training

3.4.1.29 Cisco Nexus Series 1000

How to configure a Cisco Nexus 1000V to export NetFlow v9

3.4.1.30 Cisco Nexus Series 7000

Cisco documentation on how to enable NetFlow on Nexus 7000. The following Plixer blogs also provide information on this process:

- How to configure a Nexus Series 7000
- Cisco Nexus 7000 NetFlow Sampling

3.4.1.31 Cisco Router (Cisco IOS)

Enable Cisco Express Forwarding:

```
router(config)# ip cef
```

In the configuration terminal on the router, issue the following to start NetFlow Export.

It is necessary to enable NetFlow on all interfaces through which traffic you are interested in will flow. Now, verify that the router is generating flow stats—try 'show ip cache flow'. Note that for routers with distributed switching (GSR's, 75XX's) the Rendezvous Point CLI will only show flows that made it up to the RP. To see flows on the individual linecards use the 'attach' or 'if-con' command and issue the 'show ip cache flow' on each LC.

Enable export of these flows with the global commands. 'ip flow-export source' can be set to any interface, but the one which is the least likely to enter a 'down' state is preferable. NetFlow will not be exported if the specified source is down. For this reason, we suggest the Loopback interface, or a stable Ethernet interface:

```
router(config)# ip flow-export version 5
router(config)# ip flow-export destination
router(config)# ip flow-export source FastEthernet0
```

Use the IP address of your NetFlow Collector and configured listening port.

If your router uses BGP protocol, you can configure AS to be included in exports with command:

```
router(config)# ip flow-export version 5 [peer-as | origin-as]
```

The following commands break up flows into shorter segments.

```
router(config)# ip flow-cache timeout active 1
router(config)# ip flow-cache timeout inactive 15
```

Use the commands below to enable NetFlow on each physical interface (i.e. not VLANs and Tunnels, as they are auto included) you are interested in collecting a flow from. This will normally be an Ethernet or WAN interface. You may also need to set the speed of the interface in kilobits per second. It is especially important to set the speed for frame relay or ATM virtual circuits.

```
interface
ip route-cache flow
bandwidth
```

Now write your configuration with the 'write' or 'copy run start' commands. When in enabled mode, you can see current NetFlow configuration and state with the following commands:

```
router# show ip flow export
router# show ip cache flow
router# show ip cache verbose flow
```

3.4.1.32 Cisco Wireless LAN Controller

Cisco WLC NetFlow Configuration

3.4.1.33 Cisco Zone-Based Firewall

Cisco Zone-Based Firewall Logging Support

3.4.1.34 ESX Server running VMware

Enabling NetFlow on Virtual Switches

3.4.1.35 Exinda Router

how to configure an Exinda Router

3.4.1.36 Extreme (Enterasys) N-series DFE/S-series (native NetFlow in ASIC)

DFE and S series netflow commands

```
set netflow export-interval 1
set netflow export-destination 2055
```

Enable NetFlow on each type of interface on the switch. For example:

```
set netflow port fe.*.* enable
set netflow port ge.*.* enable
set netflow port tg.*.* enable
set netflow port lag.*.* enable
set netflow cache enable
```

(continues on next page)

(continued from previous page)

```
set netflow export-version 9
set netflow template refresh-rate 50 timeout 1
```

NOTE: There is no performance impact to the switch because the flow creation and accounting is a native function of the ASIC. For more information, please refer to our "How to Enable NetFlow on an Enterasys SSR" guide.

3.4.1.37 Extreme Networks Router

To enable the flow statistics feature on a switch, use the following command:

```
enable flowstats
```

The flow statistics feature is disabled by default.

To disable the flow statistics feature on a switch, use the following command:

```
disable flowstats
```

To enable the flow statistics function on the specified port, use the following command:

```
enable flowstats ports
```

The flow statistics function is disabled by default.

To disable the flow statistics function on the specified port, use the following command:

```
disable flowstats ports
```

A single port can distribute statistics across multiple groups of flow-collector devices. This NetFlow distribution capability makes it possible to create a collection architecture that scales to accommodate high volumes of exported data. It also offers a health-checking function that improves the reliability of the collection architecture by ensuring that only responsive flow-collector devices are included in active export distribution lists. The distribution algorithm also ensures that all the ingress flow records for a given flow are exported to the same collector.

NetFlow distribution is enabled by configuring export distribution groups that identify the addresses of multiple flow-collector devices. You can configure up to 32 export distribution groups on a BlackDiamond 6800 series switch, and each group can contain as many as eight flow-collector devices.

To configure the export groups and flow-collector devices to which NetFlow datagrams are exported, use the following command:

```
config flowstats export <group#> [add | delete] [ | ] port
```

The group# parameter is an integer in the range from 1 through 32 that identifies the specific group for which the destination is being configured.

You can use the add and delete keywords to add or delete flow-collector destinations.

To export NetFlow datagrams to a group, you must configure at least one flow-collector destination. By default, no flow-collector destinations are configured. To configure a flow-collector destination, use either an IP address and UDP port number pair or a hostname and UDP port number pair to identify the flow-collector device to which NetFlow export datagrams are to be transmitted. You can configure up to eight flow-collector destinations for each group. When multiple flow-collectors are configured as members of the same group, the exported NetFlow datagrams are distributed across the available destinations.

To configure the IP address that is to be used as the source IP address for NetFlow datagrams to be exported, use the following command:

```
config flowstats source
```

By default, flow records are exported with the VLAN interface address that has a route to the configured flow-collector device. Depending on how it is configured, a flow-collector device can use the source IP address of received NetFlow datagrams to identify the switch that sent the information.

The following command example specifies that the IP address 192.168.100.1 is to be used as the source IP address for exported NetFlow datagrams.

```
config flowstats source 192.168.100.1
```

Flow records are exported on an age basis. If the age of the flow record is greater than the configured time-out, the record is exported.

To configure the time-out value for flow records on the specified port, use the following command:

```
config flowstats timeout ports [ | any]
```

The time-out value is the number of minutes to use in deciding when to export flow records. The default time-out is 5 minutes.

The following command example specifies a 10-minute time-out for exported NetFlow datagrams on port 1 of the Ethernet module installed in slot 8 of the BlackDiamond switch.

```
config flowstats timeout 10 ports 8:1
```

To reset the flow statistics configuration parameters for a specified Ethernet port to their default values, use the following command:

```
unconfig flowstats ports
```

To display status information for the flow statistics function, use the following command:

```
show flowstats {detail | group <group#> | ports }
```

where:

1. **detail** Use this optional keyword to display detailed NetFlow configuration information.
2. **group#** Use this optional parameter with the group keyword to display status information for a specific export group.
3. **portlist** Use this optional parameter to specify one or more ports or slots and ports for which status information is to be displayed.

If you enter the show flowstats command with none of the optional keywords or parameters, the command displays a summary of status information for all ports.

The summary status display for a port shows the values for all flow statistics configuration parameters for the port.

The summary status display for an export group includes the following information:

- Values for all configuration parameters
- Status of each export destination device

The detailed status display for an export group includes the summary information, plus the following management information:

- Counts of the number of times each flow collector destination has been taken out of service due to health-check (ping check) failures

- The source IP address configuration information

For more information, please refer to Extreme Networks documentation and support at http://www.extremenetworks.com

3.4.1.38 Extreme S-Series, N-Series, and K-Series

Extreme NetFlow configuration for S-Series, N-Series, and K-Series

3.4.1.39 Fatpipe Wrap

Fatpipe Warp NetFlow Support

3.4.1.40 Fortiswitch-500

Fortiswitch IPFIX configuration

3.4.1.41 HP 9300

HP 9300 NetFlow configuration

3.4.1.42 Ixia Appliance

Ixia IPFIX configuration

3.4.1.43 Juniper Router

EX-series Switches.

Juniper supports flow exports by sampling packet headers with the routing engine and aggregating them into flows. Packet sampling is achieved by defining a firewall filter to accept and sample all traffic, applying that rule to an interface, and then configuring the sampling forwarding option.

```
interfaces {
ge - 0 / 1 / 0 {
  unit 0 {
    family inet {
      filter {
        input all;
        output all;
      }
      address / (
      }
    }
  }
}
firewall {
  filter all {
    term all {
      then {
```

(continues on next page)

(continued from previous page)

```
        sample;
        accept;
      }
    }
  }
}
forwarding - options {
  sampling {
    input {
      family inet {
        rate 100;
      }
    }
    output {
      cflowd {
        port;
        version;
      }
    }
  }
}
```

For more information on configuring Juniper routers, refer to: http://www.juniper.net.

3.4.1.44 Meraki

Meraki NetFlow Support

3.4.1.45 MikroTik Router

Below are examples of how to enable Traffic-Flow on a router.

Enable Traffic-Flow on the router:

```
[admin@MikroTik] ip traffic-flow> set enabled=yes
[admin@MikroTik] ip traffic-flow> print
enabled: yes
interfaces: all
cache-entries: 1k
active-flow-timeout: 1m
inactive-flow-timeout: 15s
[admin@MikroTik] ip traffic-flow>
```

Specify IP address and port of the host, which will receive Traffic-Flow packets:

```
[admin@MikroTik] ip traffic-flow target>
add address=192.168.0.2:2055 \
\... version=9
[admin@MikroTik] ip traffic-flow target> print
Flags: X - disabled
# ADDRESS VERSION
```

(continues on next page)

(continued from previous page)

```
0 192.168.0.2:2055 9
[admin@MikroTik] ip traffic-flow target>
```

For further information see our blog MikroTik NetFlow Support.

3.4.1.46 Palo Alto Firewall

How to configure a Palo Alto Device

3.4.1.47 pfSense Firewall

Exporting NetFlow data with softflowd

3.4.1.48 Riverbed Steelhead Appliance

```
(config)# ip flow-export destination interface
(config)# ip flow-export enable
```

View more Steelhead commands.

3.4.1.49 Silver Peak WAN Optimizer

How to configure a Silver Peak WAN Optimizer

3.4.1.50 Softflowd Netflow Probe

How to configure softflowd

3.4.1.51 Sophos Cyberoam

How to configure a Sophos Cyberoam

3.4.1.52 Talari Appliance

Talari NetFlow Support

3.4.1.53 Velocloud Appliance

Velocloud IPFIX Support

3.4.1.54 Viavi Observer GigaStor

Viavi Observer GigaStor NetFlow Support

3.4.1.55 vSphere 5 Server and want to use vMotion on multiple network adapters

Watch the video here, it explains the NetFlow piece starting at ~10.20.

Learn how to enable NetFlow on vSphere

3.4.1.56 vSwitch

How to configure a vSwitch

3.4.1.57 Vyatta Core 6 software

Configuration

```
system {
accounting {
  interface {#
    multi - value sampling - rate# sample 1 in N packets,
      default
  }
  syslog - facility facility netflow {
    version < 1 | 5 | 9 > #
      default 5 engine - id# 0 - 255 server {#
        multi - value port#
      }
    timeout {
      expiry - interval#
      default 60 flow - generic#
      default 3600 icmp#
      default 300 max - active - life#
      default 604800 tcp - fin#
      default 300 tcp - generic#
      default 3600 tcp - rst#
      default 120 udp#
      default 300
    }
  }
  sflow {
    agentid server {#
      multi - value port#
      default 6343
    }
  }
}
```

3.4.2 sFlow Configurations

3.4.2.1 Alcatel Switch

Enter your Scrutinizer server information:

```
sflow receiver 1 name address udp-port packet-size 1400 version 5 timeout 0
```

Receiver Name can be set to any one-word string you want (e.g. Scrutinizer). Port should be set to 2055 by default. Packet-size should be set to 1400, version should be 5, and timeout should be 0.

Next, configure a sampler on all desired interfaces:

```
sflow sampler 1 receiver 1 rate 1 sample-hdr-size 128
```

So, if you wanted to configure ports 18 and 35 to sample for a switch with a single blade and 48 ports, you would enter:

```
sflow sampler 1 1/18 receiver 1 rate 1 sample-hdr-size 128
sflow sampler 1 1/35 receiver 1 rate 1 sample-hdr-size 128
```

Finally, configure one poller to get sFlow counters:

```
sflow poller 1 receiver 1 interval 5
```

Write configuration to switch:

```
write memory
```

3.4.2.2 Arista Switch

Arista sFlow support

3.4.2.3 Blue Coat Packeteer Packet Shaper of Proxy

Blue Coat NetFlow Support

3.4.2.4 Brocade ICX series

I found that this config works on the MLXe series of routers and some ICX. sFlow is sampled NetFlow and with Brocade the sample rate is dependent on the interface speed. With a higher sample rate, we will not see as granular data as we would with regular NetFlow. We recommend getting as close to 1 as possible for the best data. This may not be ideal for some users. Please keep in mind the current workload on your device before setting your sample rate to 1 to 1.

Sample Config:

```
(config)# interface ethernet 1/1 to 1/8fgs
(config-mif-0/1/1-0/1/24)# sflow forwarding
(config-mif-0/1/1-0/1/24)# exit
(config)# sflow destination <Scrutinizer's IP Address> 2055
(config)# sflow sample <value 1 to X>
```

Link speed	Sampling Rate
10 Mb/s	1 out of 200
100Mb/s	1 out of 500
1 Gb/s	1 out of 1000
10 Gb/s	1 out of 2000

```
(config)# sflow polling-interval 30
(config)# sflow enable
```

You can also use the following command to list the configuration settings:

```
fgs# show sflow
```

I have found this configuration consistent across all of the MLXe series devices,along with compatibility with the ICX series (formerly Ruckus).

3.4.2.5 Brocade MLXe series

I found that this config works on the MLXe series of routers and some ICX. sFlow is sampled NetFlow and with Brocade the sample rate is dependent on the interface speed. With a higher sample rate, we will not see as granular data as we would with regular NetFlow. We recommend getting as close to 1 as possible for the best data. This may not be ideal for some users. Please keep in mind the current workload on your device before setting your sample rate to 1 to 1.

Sample Config:

```
(config)# interface ethernet 1/1 to 1/8fgs
(config-mif-0/1/1-0/1/24)# sflow forwarding
(config-mif-0/1/1-0/1/24)# exit
(config)# sflow destination <Scrutinizer's IP Address> 2055
(config)# sflow sample <value 1 to X>
```

Link speed	Sampling Rate
10 Mb/s	1 out of 200
100Mb/s	1 out of 500
1 Gb/s	1 out of 1000
10 Gb/s	1 out of 2000

```
(config)# sflow polling-interval 30
(config)# sflow enable
```

You can also use the following command to list the configuration settings:

```
fgs# show sflow
```

I have found this configuration consistent across all of the MLXe series devices,along with compatibility with the ICX series (formerly Ruckus).

3.4.2.6 Cisco Nexus 3000

For information on enabling sFlow on a Cisco Nexus 3000, view the Cisco Nexus configuration guide.

3.4.2.7 Cisco UCS server

How to configure NetFlow on Cisco UCS

3.4.2.8 Cumulus Networks OS

Cumulus Networks sFlow Configuration

3.4.2.9 Dell switch

Review the following sFlow setup guides depending on which series router you have:

- 6000 series
- EX 4200

3.4.2.10 D-Link DGS-3627 or DGS-3650 switch

For information on enabling sFlow on supported D-Link switches, please review the sFlow section of the DGS-36XX User Manual V2.00, as well as our D-Link sFlow Configuration Guide.

3.4.2.11 Extreme (Enterasys) B3/C3/G3/B5/C5 Series switch

sFlow is only supported on Enterasys B3/C3/G3 series switches running firmware 6.3.1 or above. For information on enabling sFlow on these supported Enterasys® switches, please review the sFlow section of the Enterasys® SecureStack™ Configuration Guide, beginning on page 28-4.

Example Configuration for B5/C5 SecureStack™ hardware

The general procedure for configuring sFlow includes:

1. Configure your sFlow Collector information to be used by the sFlow Agent on the switch. Up to eight Collectors can be configured. The information is stored in the sFlowReceiverTable.
2. Enable and configure sFlow packet flow sampling instances on each port.
3. Enable and configure sFlow counter sampling poller instances on each port.

The following is an example of the commands used to configure sFlow:

configure sFlow Collector 1 accept defaults for datagram size and port

```
set sflow receiver 1 owner enterasys timeout 180000
set sflow receiver 1 ip 192.168.16.91
```

configure packet sampling instances on ports 1 through 12 assign to sFlow Collector 1

```
set sflow port ge.1.1-12 sampler 1
set sflow port ge.1.1-12 sampler maxheadersize 256
set sflow port ge.1.1-12 sampler rate 2048
```

configure counter poller instances on ports 1 through 12 assign to sFlow Collector 1

```
set sflow port ge.1.1-12 poller 1
set sflow port ge.1.1-12 poller interval 20
```

3.4.2.12 ExtremeXOS Switch

View the PDF Guide, which references the commands to configure sFlow on Extreme Switches.

For more Extreme commands, view the ExtremeWare Command Reference Guide.

3.4.2.13 Force10 Switch or Router

The following commands configure a Force10 switch/router with IP address 1.1.2.2 to sample at 1-in-512 and send the sFlow packets to Scrutinizer with IP address 1.1.1.1 over UDP port 6343:

```
Force10(conf)#sflow collector 1.1.1.1 agent-addr 1.1.2.2
Force10(conf)#sflow sample-rate 512
Force10(conf)#sflow enable
```

sFlow must then be enabled on every interface that should be sampled:

```
Force10(conf-if-gi-0/0)#sflow enable
```

To list the configuration settings use the command:

```
Force10#show sflow
```

```
sFlow services are enabled
Global default sampling rate: 512
Global default counter polling interval: 20
Global extended information enabled: none
1 collectors configured
Collector IP addr: 1.1.1.1, Agent IP addr: 1.1.2.2, UDP port: 6343
20088 UDP packets exported
0 UDP packets dropped
3940 sFlow samples collected
0 sFlow samples dropped due to sub-sampling
Linecard 0 Port set 0 H/W sampling rate 512
Gi 0/0: configured rate 512, actual rate 512, sub-sampling rate 1
```

3.4.2.14 Fortinet Firewall

Read the Would you like to have some traffic visibility on your Fortinet Firewall? blog to get NetFlow setup instructions for the Fortinet Firewall.

3.4.2.15 Foundry Switch

There are only 3 commands to enable sFlow on Foundry gear.

Enable it globally

```
(config)# sflow enable
```

Configure a destination

```
(config)# sflow destination x.x.x.x
```

Enable it on port(s)

```
(config)# interface eth 1 (or for multiple ports (config)# interface eth 1 to 48)
(config-if-1)# sflow forwarding
```

For more Foundry commands, view the Foundry Command Reference Guide.

3.4.2.16 H3C MSR Series Router

View the 02-IP Services Volume(V1.05) Command Manual, which details the commands to configure sFlow on H3C MSR Series Routers.

3.4.2.17 H3C S12500 Series Switch

View the 13-Network Management and Monitoring Command Reference, which shows how to setup sFlow on H3C S12500 Series Routers.

3.4.2.18 H3C S5500-E1 or S7500-E Series Switch

View the PDF Guide, which references the commands to configure sFlow on H3C supported equipment.

3.4.2.19 HP Procurve Switch 2800 or 5300 series

IMPORTANT:

2800 Series must be running Software Revision I.08.105 and Firmware (ROM) version I.08.07 5300 Series must be running Software Revision E.10.37 or higher

For information on enabling sFlow on 2800 or 5300 series HP Procurve Switches, download this ZIP fileand review the PDF inside for further instructions.

3.4.2.20 HP Procurve Switch 5400, 3500 or 8200 series - running K code

HP has added support for configuring sFlow directly on the CLI.

From config mode:

Configure destination collector

```
sflow [1-3] destination [IP-addr] [udp-port-for-sflow]
```

Where 1-3 is the sFlow instance, IP-addr is the address of the Scrutinizer collector, and udp-port-for-sflow is the number of the listening port of the collector. example:

```
sflow 1 destination 192.168.1.1 6343
```

Activate Sampling

```
sflow [1-3] sampling [ports list] [N]
```

Where 1-3 is the sFlow instance, ports list is the port(s) setup for sFlow, and N is the number of sampled packets (to sample every 100 packets set N to 100). example:

```
sflow 1 sampling all 100
```

Activate Polling

```
sflow [1-3] polling [ports list] [N]
```

Where 1-3 is the sFlow instance, ports list is the port(s) setup for sFlow, and N is the number of interval (in seconds) between polling intervals. example:

```
sflow 1 polling all 60
```

Save Configuration

```
write mem
```

3.4.2.21 HP Procurve Switch 5400zl, 3500yl and 6200yl

For information on enabling sFlow on supported HP Procurves, view the ProCurve Networking FAQ.

3.4.2.22 Juniper Switch or Router

For instructions on how to enable sFlow on supported Juniper routers and switches, please review Configuring sFlow Technology for Network Monitoring (CLI Procedure).

3.4.2.23 Juniper EX 3200 switch

The following configuration enables sFlow monitoring of all interfaces on a Juniper EX3200 switch, sampling packets at 1-in-500, polling counters every 30 seconds and sending the sFlow to an analyzer (10.0.0.50) on UDP port 6343 (the default sFlow port).

```
protocols {
sflow {
  polling - interval 30;
  sample - rate 500;
  collector 10.0 .0 .50 {
    udp - port 6343;
  }
  interfaces ge - 0 / 0 / 0.0;
  interfaces ge - 0 / 0 / 1.0;
  interfaces ge - 0 / 0 / 2.0;
```

(continues on next page)

(continued from previous page)

```
    interfaces ge-0/0/3.0;
    interfaces ge-0/0/4.0;
    interfaces ge-0/0/5.0;
    interfaces ge-0/0/6.0;
    interfaces ge-0/0/7.0;
    interfaces ge-0/0/8.0;
    interfaces ge-0/0/9.0;
    interfaces ge-0/0/10.0;
    interfaces ge-0/0/11.0;
    interfaces ge-0/0/12.0;
    interfaces ge-0/0/13.0;
    interfaces ge-0/0/14.0;
    interfaces ge-0/0/15.0;
    interfaces ge-0/0/16.0;
    interfaces ge-0/0/17.0;
    interfaces ge-0/0/18.0;
    interfaces ge-0/0/19.0;
    interfaces ge-0/0/20.0;
    interfaces ge-0/0/21.0;
    interfaces ge-0/0/22.0;
    interfaces ge-0/0/23.0;
  }
}
```

Visit blog.sFlow.com for more information on configuring sFlow on Juniper switches.

3.4.2.24 ZyXEL Appliance

ZyXEL sFlow configuration

3.4.3 NetStream Configurations

3.4.3.1 3com Router or Switch

NetFlow (AKA NetStream) is supported on the 5000 & 6000 routers via a software upgrade and on the 8800 Switch via an NMM module.

To configure NetStream on a 3Com 5012 router, use the following sample configuration:

```
ip netstream export source interface
ip netstream export host
```

Then activate NetStream on each specific interface you want to obtain statistics from. For example, on the Serial0/0 interface, use the following command.

```
interface s0/0
ip netstream inbound
```

This will export inbound NetStream traffic statistics related to the Serial0/0 interface of the 3com router to the workstation running Scrutinizer.

3.4.4 IPFIX Configuration

3.4.4.1 Avaya Router

Avaya IPFIX Support

3.4.4.2 Avaya WLAN 8100 Wireless Controller

Avaya Wireless 8100 IPFIX Configuration

3.4.4.3 Barracuda Firewall

Barracuda IPFIX Support

3.4.4.4 Blue Coat Crossbeam Appliance

Blue Coat Crossbeam configuration

3.4.4.5 Brocade 5600 vRouter

Brocade 5600 IPFIX Configuration

3.4.4.6 Cisco NGA 3240

Visit the command reference page or click here

3.4.4.7 Citrix NetScaler sending AppFlow (IPFIX)

You can configure IPFIX on your Citrix NetScaler device using this setup guide.

3.4.4.8 Ecessa Appliance

Ecessa Appliances

3.4.4.9 Emulex EndaceFlow 3040

Emulex NetFlow Support

3.4.4.10 EndaceFlow 4004

Endace NetFlow Support

3.4.4.11 Extreme Switch

IPFIX support is available on the BlackDiamond 8900 G96Tc, G48T-xl, G48X-xl, and 10G8X-xl modules and Summit X460 and X480 switches.

To configure whether to meter on ingress and/or egress ports, use the following command:

```
configure ip-fix ports [ingress \| egress \| ingress-and-egress]
# The default is ingress.
```

To configure whether to meter all, dropped only, or non-dropped only records, use the following command:

```
configure ip-fix ports record [all \| dropped-only \| non-dropped]
# The default is all
```

3.4.4.12 F5 Networks Big-IP System

This configuration guide

3.4.4.13 Fortinet Switch

Fortinet IPFIX Support

3.4.4.14 Gigamon Appliance

These blogs provide information on the process.

- Gigamon NetFlow Support
- Gigamon IPFIX Configuration
- Gigamon NetFlow Configuration From Command Line

3.4.4.15 IBM Proventia Network Intrusion Prevention Appliance

IBM Proventia IPFIX Support

3.4.4.16 Juniper MX240, MX480 or MX960 running JUNOS Release 10.2

To configure inline flow monitoring, include the inline-jflow statement at the [edit forwarding-options sampling instance instance-name family inet output] hierarchy level. Inline sampling exclusively supports a new format called version-ipfix that uses UDP as the transport protocol. When you configure inline sampling, you must include the version-ipfix statement at the [edit forwarding-options sampling instance instance-name family inet output flow-server address] hierarchy level and also at the [edit services flow-monitoring] hierarchy level.

The following operational commands include new inline fpc keywords to display inline configuration information: show services accounting errors, show services accounting flow, and show services accounting status.

To learn more click here for a listing (and description) of all features that have been added to JUNOS Release 10.2.

3.4.4.17 Juniper MX series post release 14.1X55

Juniper MX IPFIX Reporting

3.4.4.18 Juniper vMX

Juniper vMX IPFIX Support

3.4.4.19 Microsoft Event Logs

Monitoring failed login attempts with IPFIX

3.4.4.20 Nortel ERS 5500 & 8600 series routers

This Configuration Guide shows how to enable IPFIX using Java Device Manager (JDM) or with the Command Line Interface. (See Chapter 4).

NOTE: The 5500 series only supports IP packet sampling resulting in lower than actual utilization trends.

Utilization can be understated on Nortel IPFIX capable equipment. To fix this issue, review the hash overflow document.

3.4.4.21 nProbe

How to configure nProbe NetFlow IPFIX

3.4.4.22 Open vSwitch

This document on Open vSwitch explains the process

3.4.4.23 Procera Appliance

Procera IPFIX Support

3.4.4.24 Saisei Networks Appliace

Saisei IPFIX Support

3.4.4.25 Solera DeepSee Appliance

Solera IPFIX support

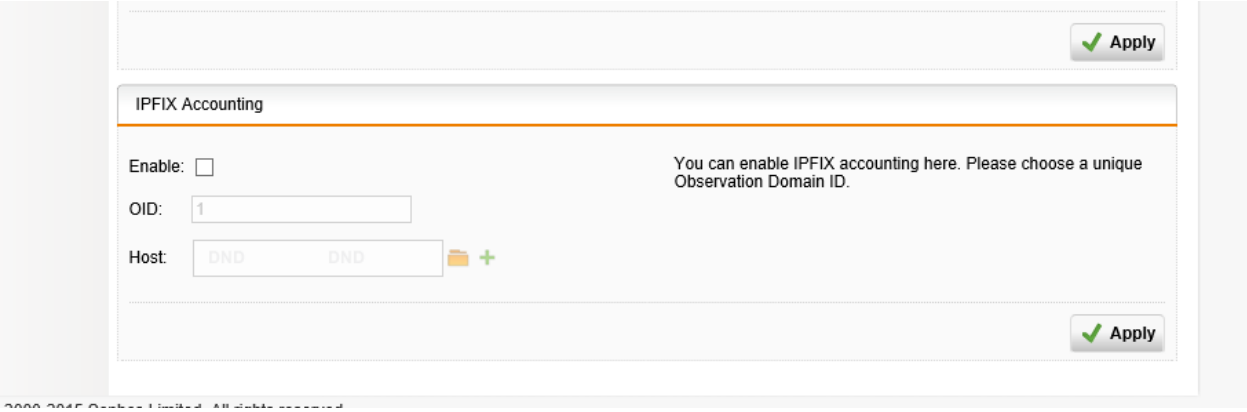
3.4.4.26 SonicWALL

The current supported models are TZ210, NSA240, 2400, 3500, 4500, 5000, NSA E-5500, 6500, 7500, 8500 running 5.8.0.1 or later.

Read the SonicWALL documentation on NetFlow and IPFIX support.

3.4.4.27 Sophos UTM Firewall

Configuring IPFIX on your Sophos UTM is done by enabling the IPFIX Accounting Feature.



Read the Sophos documentation on IPFIX support. Page 126 outlines the IPFIX accounting feature.

3.4.4.28 Stormshield Appliance

Stormshield IPFIX Support

3.4.4.29 Ubiquiti Appliance

Ubiquiti NetFlow support

3.4.4.30 Viptela Appliance

Viptela IPFIX Support

3.4.4.31 VMware DFW (Distributed Firewall)

VMware DFW IPFIX Support

3.4.4.32 VMware Virtual Distributed Switch (VDS)

VMware IPFIX Support

3.4.4.33 VMware vSphere ESX

VMware ESX support

3.4.4.34 Xirrus Wireless Access Point

Xirrus IPFIX support

3.4.4.35 YAF Flow Probe

YAF probe

3.4.5 jFlow Configurations

3.4.5.1 Juniper SRX Series Gateway

Configure J-Flow on a Juniper SRX

3.4.5.2 Juniper SRX100H

Juniper SRX100H NetFlow Support