

## ADS Integration With Log Management

Flowmon ADS solution is ready for integration with many types of Log Management tools. This document describes 3 scenarios of how to integrate Log Management tools with Flowmon ADS solution. First scenario is based on Syslog exported in CEF file format. Second scenario allows link from Flowmon ADS to your system and last option is able to link your system with Flowmon ADS.

### 1. Event Exporting from Flowmon ADS to Log manager

Event export from Flowmon ADS to Log manager is going through Syslog. Event export is available in CEF file format.

#### Configuration

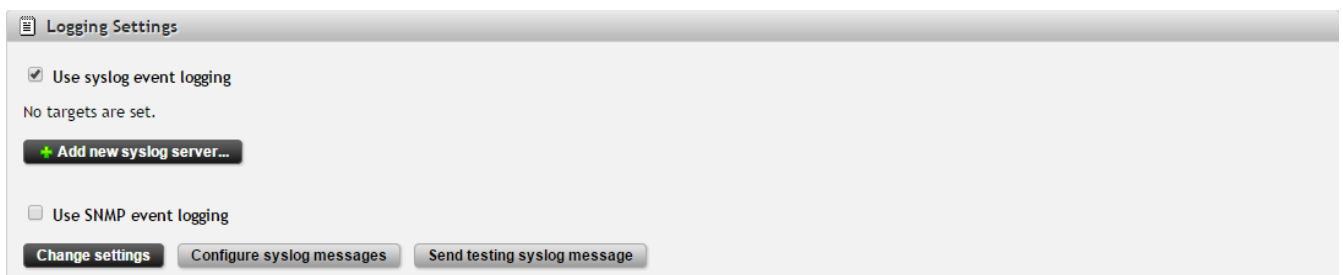
Flowmon ADS > Configuration > Traffic processing > tab Event reporting > Syslog



**Important:** Tick the EventID checkbox for sending unique EventID for event reporting.

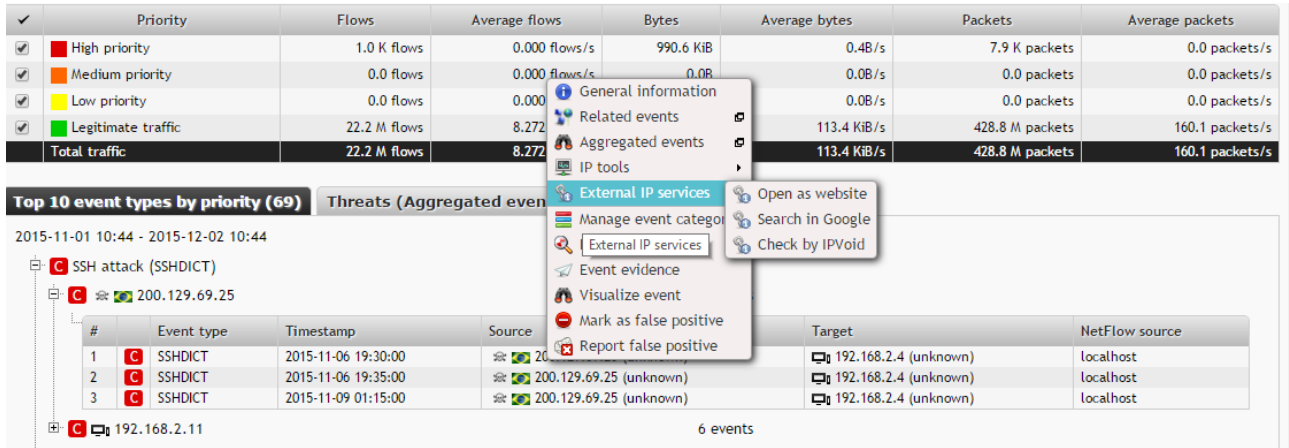
#### Syslog Sending

Flowmon Configuration Center > System > System settings > section Logging settings



## 2. Link from Flowmon ADS to Your System

You can use your own link to another system. Right click on event and select External IP services.



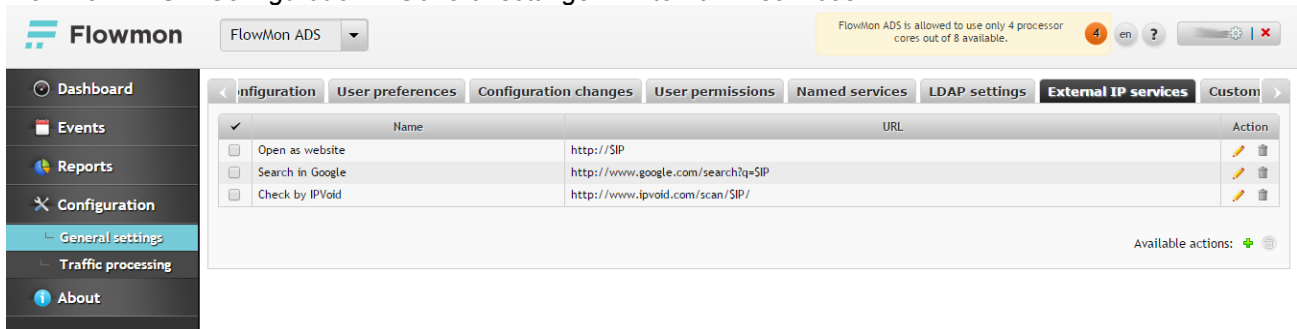
Priority	Flows	Average flows	Bytes	Average bytes	Packets	Average packets
High priority	1.0 K flows	0.000 flows/s	990.6 KiB	0.4B/s	7.9 K packets	0.0 packets/s
Medium priority	0.0 flows	0.000 flows/s	0.0B	0.0B/s	0.0 packets	0.0 packets/s
Low priority	0.0 flows	0.000		0.0B/s	0.0 packets	0.0 packets/s
Legitimate traffic	22.2 M flows	8.272		113.4 KiB/s	428.8 M packets	160.1 packets/s
<b>Total traffic</b>	<b>22.2 M flows</b>	<b>8.272</b>		<b>113.4 KiB/s</b>	<b>428.8 M packets</b>	<b>160.1 packets/s</b>

#	Event type	Timestamp	Source	Target	NetFlow source
1	SSHDICTION	2015-11-06 19:30:00	200.129.69.25	192.168.2.4 (unknown)	localhost
2	SSHDICTION	2015-11-06 19:35:00	200.129.69.25 (unknown)	192.168.2.4 (unknown)	localhost
3	SSHDICTION	2015-11-09 01:15:00	200.129.69.25 (unknown)	192.168.2.4 (unknown)	localhost

### Link Configuration

Flowmon ADS > Configuration > General settings > External IP services



Name	URL	Action
<input type="checkbox"/> Open as website	http://SIP	
<input type="checkbox"/> Search in Google	http://www.google.com/search?q=SIP	
<input type="checkbox"/> Check by IPVoid	http://www.ipvoid.com/scan/SIP/	

## 3. Link from Your System to Flowmon ADS

You can use link to Flowmon ADS for detail event inspection based on EventID sent to Syslog.

**Example:**

- `https://<flowmon domain>/ads/events/?_adsLink=tab*Tab.Events.SimpleList[eventDetail[0]*<EventID>`
- You must modify **domain name** of Flowmon device and use actual **EventID** (on the end of link)