

# Flowmon ADS Integration with FortiSIEM

This document explains how to configure Flowmon ADS to send events to FortiSIEM via syslog and how to configure the FortiSIEM to receive and process events properly. This guide is based on Flowmon version 10.3.7, Flowmon ADS 10.0.5 and FortiSIEM 5.2.6 (1623). It can happen that screenshots will differ in other versions of corresponding products. In that case please refer to the user guide of the respective product if needed.

## Flowmon Configuration

To send events via syslog to FortiSIEM add a new target in *Flowmon Configuration Center* section *System* part *Syslog Event Logging*. You can also adjust what groups of log messages will be sent to FortiSIEM. There is no need to send all the logs. Figure 1 shows recommended settings for syslog export and single target configured.

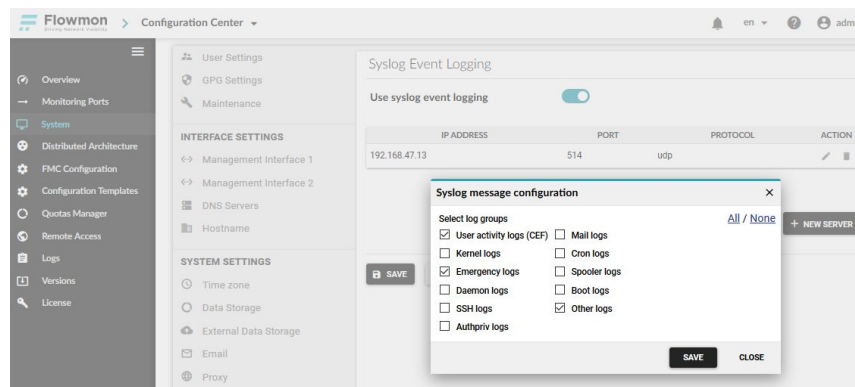


Figure 1: Configuration of event export from Flowmon via syslog

In *Flowmon ADS*, section *Settings*, tab *Processing* and part *Custom actions* there is the configuration option *Syslog message* that needs to be enabled to send events from Flowmon ADS to FortiSIEM. Events that will be exported via syslog are determined by *Perspective*. Check the option *Send one message per target* and limit the number of messages (targets) to 10. Figure 2 shows recommended settings.

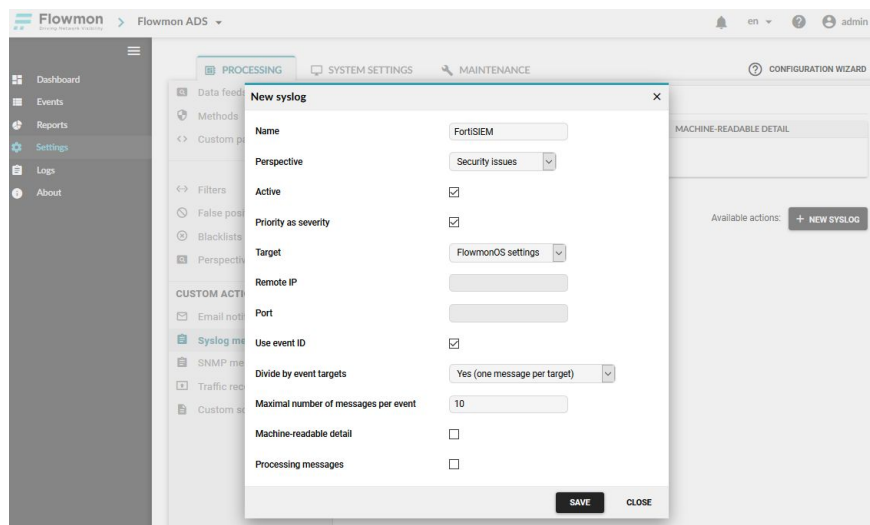
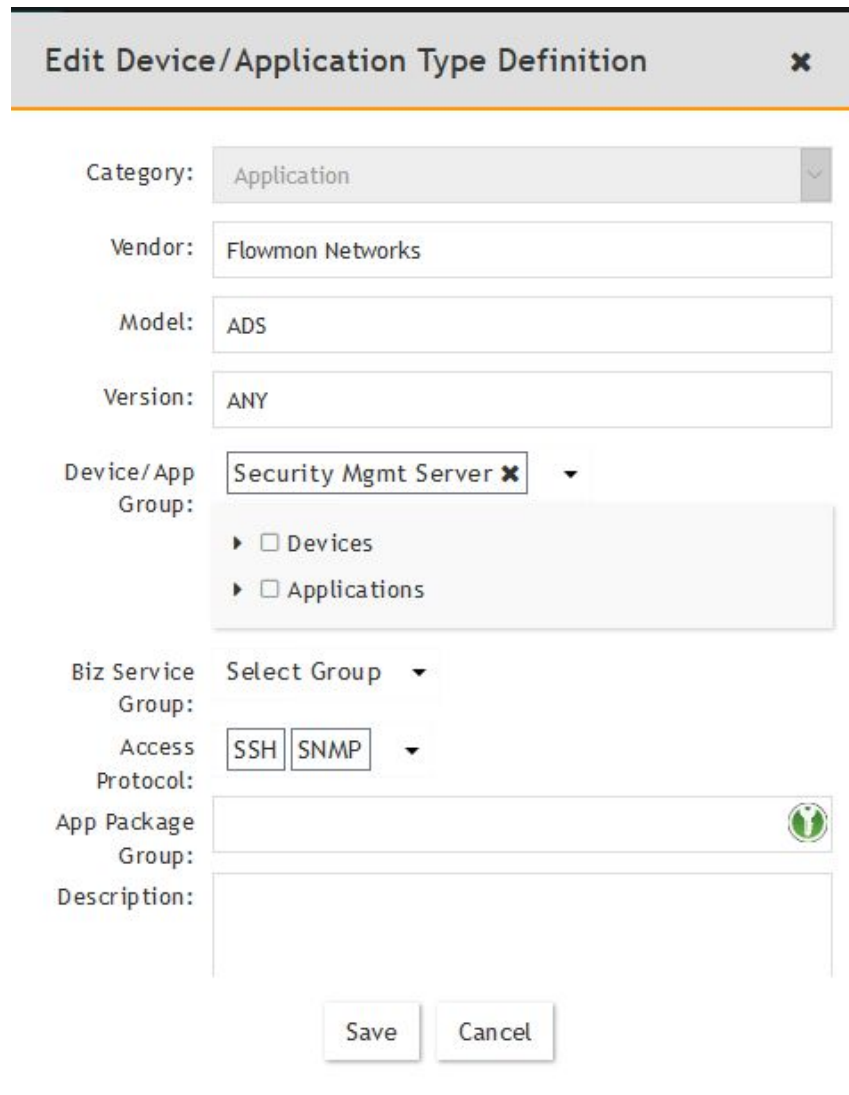


Figure 2: Recommended settings for event export to FortiSIEM via syslog

## FortiSIEM Configuration

To support Flowmon ADS in FortiSIEM go to *ADMIN > Device Support* and start by adding a new device according to example on figure 3.



**Edit Device/Application Type Definition** ✕

Category: Application

Vendor: Flowmon Networks

Model: ADS

Version: ANY


Device/App Group: Security Mgmt Server ✕

▸ ☐ Devices

▸ ☐ Applications

Biz Service Group: Select Group

Access Protocol: SSH SNMP

App Package Group: 

Description:

Save Cancel

Figure 3: Add new device in FortiSIEM

As a next step define a custom parser. It is recommended to use Google Chrome browser due to good support for copy & paste for XML like text<sup>1</sup>. To add a new parser go to *ADMIN > Device support* and in section *Parser* create a new parser according to example on figure 4. The parser itself is located in a file *Parser.XML* that is part of this integration package. Copy and paste content of the file as shown in figure 4.

<sup>1</sup> You may experience issues in other browsers, e.g. in Firefox.

Edit Event Parser Definition

Name: FlowmonADSParser

Device Type: Flowmon Networks ADS

Parser XML:

Validate

Test

Reformat

Enable

Clear Xml

Search

```

1 <patternDefinitions>
2 <pattern name="patStrEndSep"><![CDATA[["|"]]]></pattern>
3 </patternDefinitions>
4 <eventFormatRecognizer><![CDATA[["ADS:"s'CEF:"s'd+["|"](?<:patStrEndSep|)]{"s"}]]></eventFormatRecognizer>
5 <parsingInstructions>
6 <switch>
7 <case>
8 <collectFieldsByRegex src="$_rawmsg">
9 <regex><![CDATA[["gPatSyslogPRI">?{"s"<_mon:gPatMon>{"s"<_day:gPatDay>{"s"<_time:gPatTime>{"s"<_gPatStr>{"s"<_body:gPatMsgBody}}]]></regex>
10 </collectFieldsByRegex>
11 <setEventAttribute attr="deviceTime">toDate($_mon, $_day, $_time)</setEventAttribute>
12 </case>
13 <default>
14 <collectFieldsByRegex src="$_rawmsg">
15 <regex><![CDATA[ADS:"s'CEF:"s'<_body:gPatMsgBody]]></regex>
16 </collectFieldsByRegex>
17 </default>
18 </switch>
19 <setEventAttribute attr="eventType">Flowmon-ADS-Generic</setEventAttribute>
20 <when test="matches($_body, '\\\\|')">
21 <setEventAttribute attr="_body">replaceStrInStr($_body, '\\|', ":", "TEMP::")</setEventAttribute>
22 </when>
23 <setEventAttribute attr="_body">replaceStrInStr($_body, "|", ":", "SEP::")</setEventAttribute>
24 <when test="matches($_body, '.*TEMP::')">
25 <setEventAttribute attr="_body">replaceStrInStr($_body, ".*TEMP::", "|")</setEventAttribute>
26 </when>
27 <collectAndSetAttrByPos sep=":" sep::" src="$_body">
28 <attrPosMap attr="version" pos="1"/>
29 <attrPosMap attr="devVendor" pos="2"/>

```

Save

Cancel

Figure 4: Add new parser

Before saving the parser click *Validate* and *Test*. After that you will be able to save the new parser. For testing the parser you can use following sample message:

```
<179>Mar 31 09:50:26 tora ADS: CEF:0|Flowmon Networks|Flowmon ADS
Business|10.00.05|DNSANOMALY|DNS traffic anomaly|6|src=192.168.47.107
smac=00:0c:29:ee:f5:b3 start=Mar 31 2020 09:46:38 deviceCustomString1=ads.flowmon.com
deviceCustomString1Label=ADSHostName cn1=4179 cn1Label=EventID msg=Use of unauthorized
DNS server (connections: 4). target=8.8.8.8 cn2=1 cn2Label=DataFeedID cn3=4
cn3Label=PerspectiveID
```

After saving the parser click *Apply* to make sure your parser will be used for new messages. From now on, when a message is received from Flowmon ADS it will be parsed properly and displayed in *Analytics* with event name corresponding to specific event type as shown on figure 5.

Event Receive Time	Reporting IP	Event Name	Raw Event Log
Apr 16 2020, 10:50:25 AM	192.168.47.79	Flowmon-ADS-DNS-traffic-anomaly	<178>Apr 16 10:50:25 tora ADS: CEF:0 Flowmon Networks Flowmon ADS Busine
Apr 16 2020, 10:50:25 AM	192.168.47.79	Flowmon-ADS-DNS-traffic-anomaly	<178>Apr 16 10:50:25 tora ADS: CEF:0 Flowmon Networks Flowmon ADS Busine
Apr 16 2020, 10:45:25 AM	192.168.47.79	Flowmon-ADS-DNS-traffic-anomaly	<178>Apr 16 10:45:25 tora ADS: CEF:0 Flowmon Networks Flowmon ADS Busine

Figure 5: Sample events displayed in Analytics

Next and final step is to use events from Flowmon ADS in FortiSIEM workflow. Rules need to be defined to create incidents from events. Ruleset is prepared in file Rule.XML that is part of this integration package. Go to *Resources > Rules* and import file Rule.XML as shown on Figure 6. All the imported rules start with a prefix “Flowmon”.

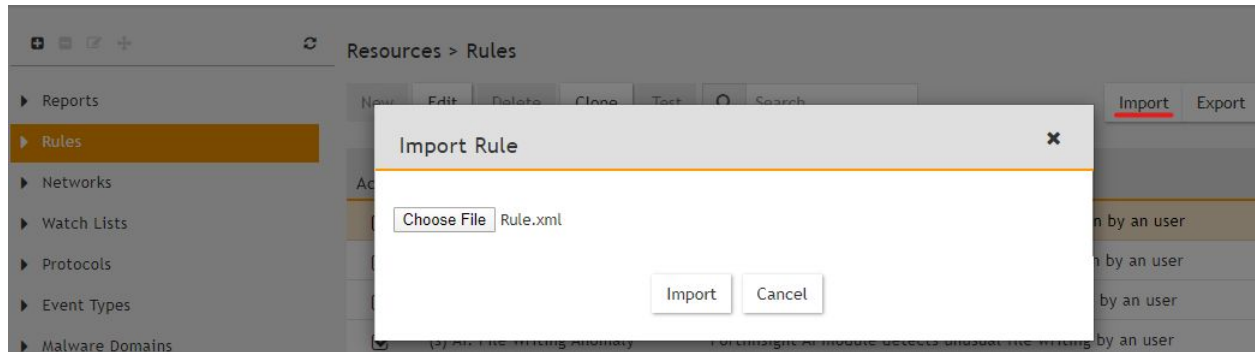


Figure 6: Rule import

You can adjust severity of incidents according to your preferences. Search for the Rule you want to modify as shown on Figure 7.

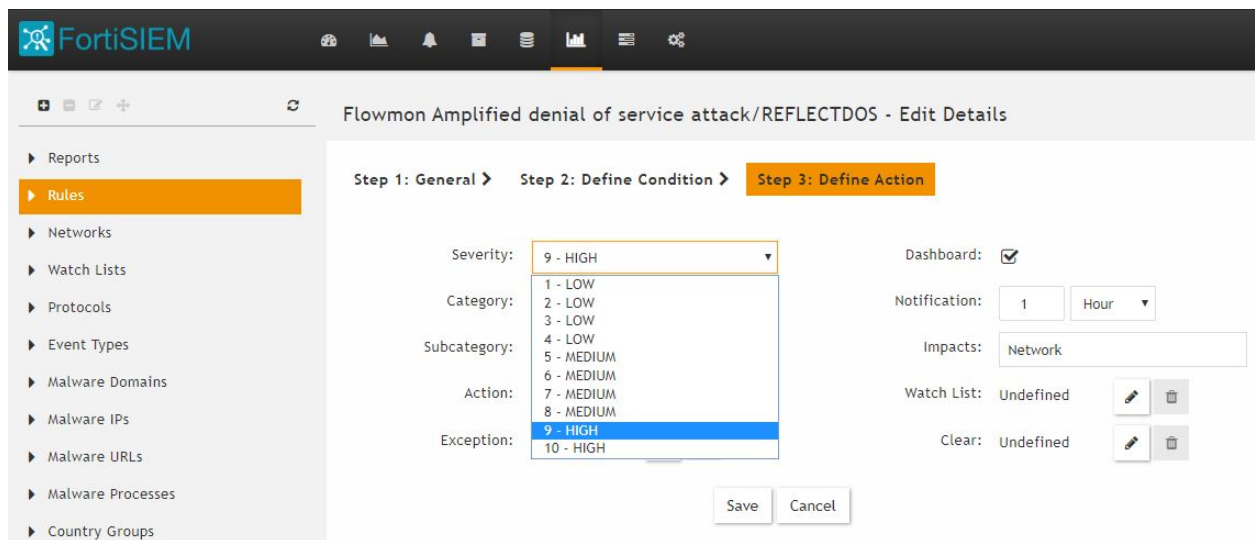


Figure 7: Rule severity modification

Integration of Flowmon ADS in FortiSIEM is completed. At this point you can create any additional workflow you are used to.