LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

LOGmanager Best Practice - Integration with Flowmon

Flowmon is focused on a network traffic and evaluates it for anomalies or attacks. Flowmon tracks how applications (including cloud), servers and users are doing in the network and whether their behaviour has changed - and notifies the administrator of possible misconduct. For an attacker, Flowmon deployed on a network is a major hurdle, because it is invisible to network traffic and cannot be easily avoided.

LOGmanager on the other hand, focuses on the information it obtains from individual devices communicating in the network. It can draw attention to possible security incidents (such as multiple failed logon attempts) and gives the opportunity to identify the operating states of end devices. Simply put, if a device or any source on the network sends information about an event, LOGmanager processes it in detail, stores it for a long time, allows it to be easily interpreted, links it to data from other systems and prevents any possible manipulation of its contents.

From this brief description, it is clear that both solutions have their place in the organization and therefore makes sense to integrate them with each other.

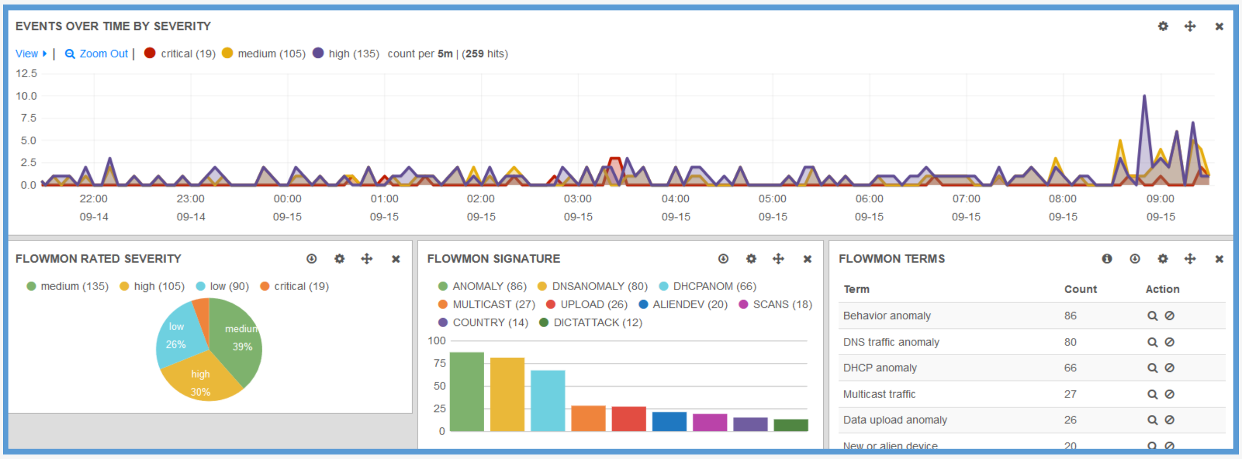
Integration possibilities

Below are the existing integration options:

1. **Collection, long-term storage and visibility into Flowmon logs in LOGmanager** - Default integration where logs from Flowmon are being sent to LOGmanager. This type of integration allows thorough processing and detailed visualization of Flowmon data in the perspective of other network and security solutions of the organization. It is easy to setup according to the instructions in the LOGmanager documentation and thanks to the built-in classification, no configuration changes are required on LOGmanager side.

2. **Enrichment of Flowmon logs processed on the LOGmanager side with additional metadata -** The built-in alerts in LOGmanager includes a sample called "Flowmon_log_enhancement". After activation it adds a new field in logs received from Flowmon, with URL link pointing to the detail of the event in the Flowmon GUI. By clicking the newly created link in the LOGmanager interface the user is redirected to the Flowmon console.

3. **Adding a user identity from Microsoft AD to the Flowmon environment** - Flowmon can receive data through its own syslog collector to enrich data it collects. More precisely - who was using given IP address, at the time of the event according to MS AD. LOGmanager obtains this information as part of the standard collection of AD logs by WES agent (LOGmanager Windows Event Sender). LM processes these logs and based on a simple logic, allows them to be passed in a structured format to Flowmon, where they are being used to enrich data.


EVENTS OVER TIME BY SEVERITY
View ▸ | Zoom Out | ● critical (19) ● medium (105) ● high (135) count per 5m | (259 hits)
12.5
10.0
7.5
5.0
2.5
0.0
22:00 09-14
23:00 09-14
00:00 09-15
01:00 09-15
02:00 09-15
03:00 09-15
04:00 09-15
05:00 09-15
06:00 09-15
07:00 09-15
08:00 09-15
09:00 09-15
FLOWMON RATED SEVERITY
● medium (135) ● high (105) ● low (90) ● critical (19)
low 26%
medium 39%
high 30%
FLOWMON SIGNATURE
● ANOMALY (86) ● DNSANOMALY (80) ● DHCPANOM (66)
● MULTICAST (27) ● UPLOAD (26) ● ALIENDEV (20) ● SCANS (18)
● COUNTRY (14) ● DICTATTACK (12)
100
75
50
25
0
FLOWMON TERMS

Term	Count	Action
Behavior anomaly	86	🔍 ⊘
DNS traffic anomaly	80	🔍 ⊘
DHCP anomaly	66	🔍 ⊘
Multicast traffic	27	🔍 ⊘
Data upload anomaly	26	🔍 ⊘
New or alien device	20	🔍 ⊘

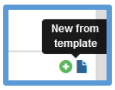
Figure: Preview of Flowmon data visualization in LOGmanager

1. Collection, long-term storage and visibility into Flowmon logs:

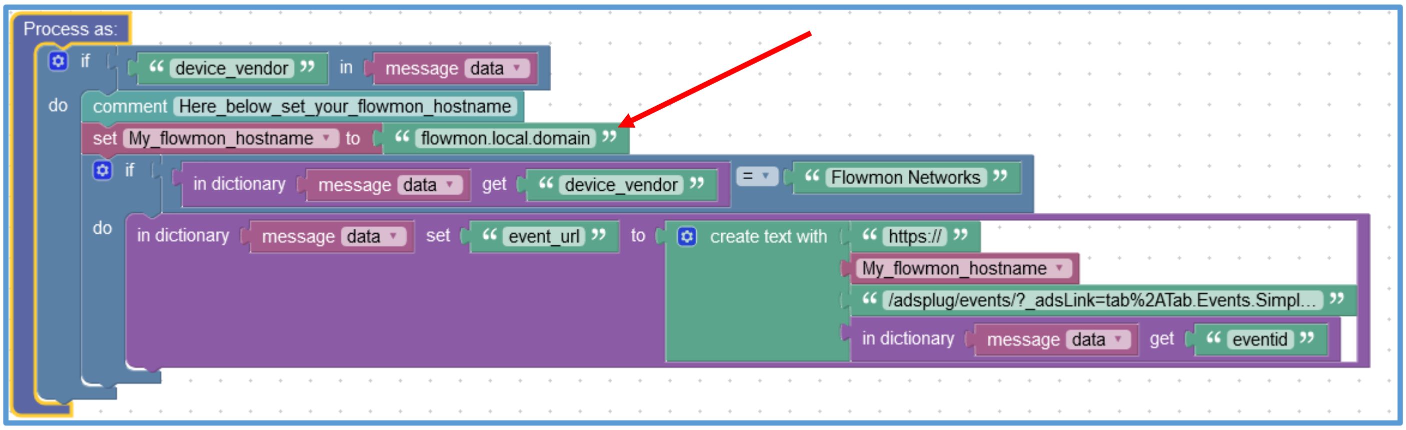
Here the integration is very easy. To achieve basic integration follow the online documentation of LOGmanager in the menu: *LOGmanager documentation / Log source devices / Flowmon*. The whole process consists of only six steps.

2. Enriching Flowmon logs with additional metadata

Procedure for enriching Flowmon ADS logs in LOGmanager with URL links of individual events:

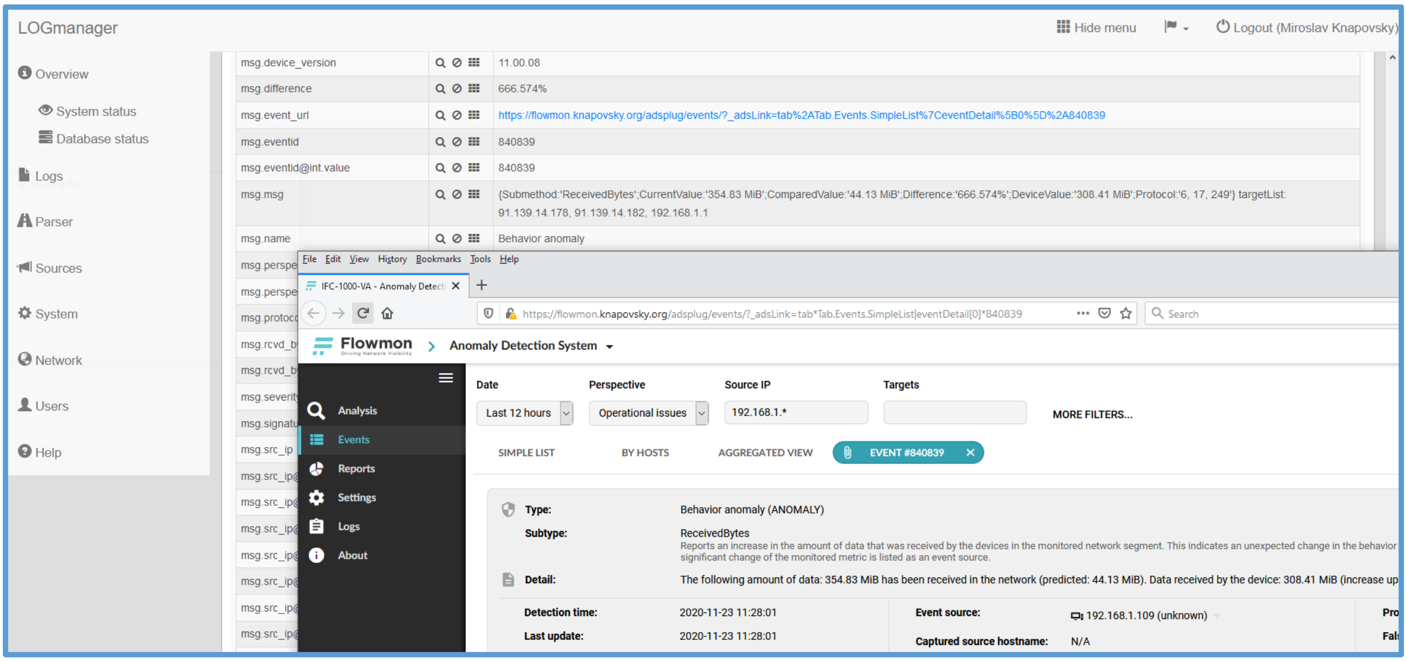


1. Create a new alert from a template - in the menu *Logs / Alerts*, click on the top-right icon - *New from template.*
2. Select one named "Flowmon_log_enhancement" from the Model Examples list and click the *Apply* button.
3. In the newly added blockly logic, edit the field indicated by the arrow in the figure below. In this field, type the domain name or IP address of your Flowmon system instead of "*flowmon.local.domain*".



```
Process as:
  if  " device_vendor "  in  message data
  do  comment Here_below_set_your_flowmon_hostname
      set My_flowmon_hostname to " flowmon.local.domain "
      if  in dictionary message data get " device_vendor "  =  " Flowmon Networks "
      do  in dictionary message data set " event_url " to  create text with  " https:// "
                                                                              My_flowmon_hostname
                                                                              " /adsplug/events/?_adsLink=tab%2ATab.Events.Simpl... "
                                                                              in dictionary message data get " eventid "
```

4. Edit the name and description and the alert as needed, fill in the email address, enable the alert and click on the "Create" button in the last step. This way you have an alert that does not warn, but adds a URL to each Flowmon ADS log. Within one minute you should find a new msg.event_url field in new incoming Flowmon logs.
5. Checking the result. Open the appropriate Flowmon event in the built-in Flowmon Dashboard, find the msg.event_url field and test whether it redirects you correctly to the given Flowmon event, as shown in the figure below.



```
msg.device_version     11.00.08
msg.difference         666.574%
msg.event_url          https://flowmon.knapovsky.org/adsplug/events/?_adsLink=tab%2ATab.Events.SimpleList%7CeventDetail%5B0%5D%2A840839
msg.eventid            840839
msg.eventid@int.value  840839
msg.msg                {Submethod:'ReceivedBytes';CurrentValue:'354.83 MiB';ComparedValue:'44.13 MiB';Difference:'666.574%';DeviceValue:'308.41 MiB';Protocol:'6, 17, 249'} targetList:
                       91.139.14.178, 91.139.14.182, 192.168.1.1
msg.name               Behavior anomaly
msg.perspe
msg.perspe
msg.protoco
msg.rcvd_b
msg.rcvd_b
msg.severit
msg.signatu
msg.src_ip
msg.src_ip
msg.src_ip
msg.src_ip
msg.src_ip
msg.src_ip
msg.src_ip
msg.src_ip
```

https://flowmon.knapovsky.org/adsplug/events/?_adsLink=tab*Tab.Events.SimpleList|eventDetail[0]*840839

Date: Last 12 hours
Perspective: Operational issues
Source IP: 192.168.1.*
Targets:

Type: Behavior anomaly (ANOMALY)

Subtype: ReceivedBytes
Reports an increase in the amount of data that was received by the devices in the monitored network segment. This indicates an unexpected change in the behavior
significant change of the monitored metric is listed as an event source.

Detail: The following amount of data: 354.83 MiB has been received in the network (predicted: 44.13 MiB). Data received by the device: 308.41 MiB (increase up

Detection time: 2020-11-23 11:28:01
Last update: 2020-11-23 11:28:01
Event source: 192.168.1.109 (unknown)
Captured source hostname: N/A
Pro
Fal

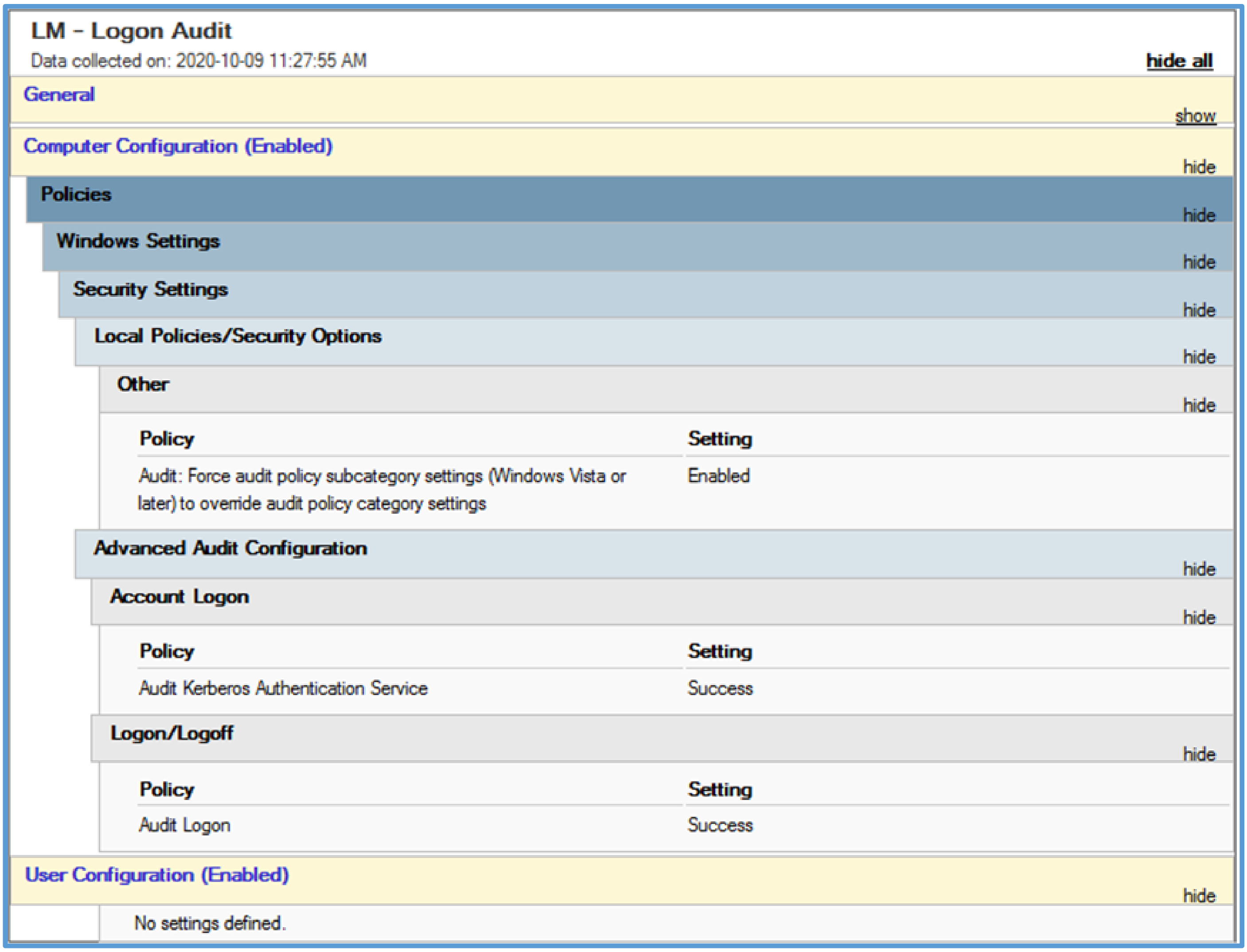
Figure: Preview of the result of creating a new field with direct link to event in Flowmon ADS

3. Addition of user identity from LOGmanager to Flowmon

The basic logic of this integration: LOGmanager can forward events associated with a successful user login to the Flowmon system. In the Flowmon system, it is then possible to connect, for example, data flows with the identity of a specific user. To successfully link the user's identity with the data flow, it is necessary to set up logging of events related to identity verification (e.g. via GPO) on domain servers, forward these events from LOGmanager to Flowmon. Flowmon must process the user identity information received from LOGmanager with a parser, which we have also prepared for you and you will find it in the manual below.

1. **GPO configuration**: The first is to create a group policy named e.g. LM - Logon Audit and connect it to the container of domain controllers and ideally also to the container of domain member servers.

   Edit the newly created group policy and in path *Computer Configuration / Policies / Windows Settings / Security Settings / Local Policies / Security Options Audit: Force audit policy subcategory settings to override audit policy category settings*, check the option *Define this policy settings,* the option *Enabled* and confirm with OK.
   Next, in path *Computer Configuration / Policies / Windows Settings / Security Settings / Advanced Audit Policy Configuration / Audit Policies / Account Logon* change the policy *Audit Kerberos Authentication Service*, check the option *Configure the following audit events*, the option *Success* and confirm with OK. Finally, in path *Computer Configuration / Policies / Windows Settings / Security Settings / Advanced Audit Policy Configuration / Audit Policies / Logon/Logoff* change the policy *Audit Logon*, check the option *Configure the following audit events,* the option *Success* and confirm with OK.



LM - Logon Audit

Data collected on: 2020-10-09 11:27:55 AM

Policy	Setting
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled

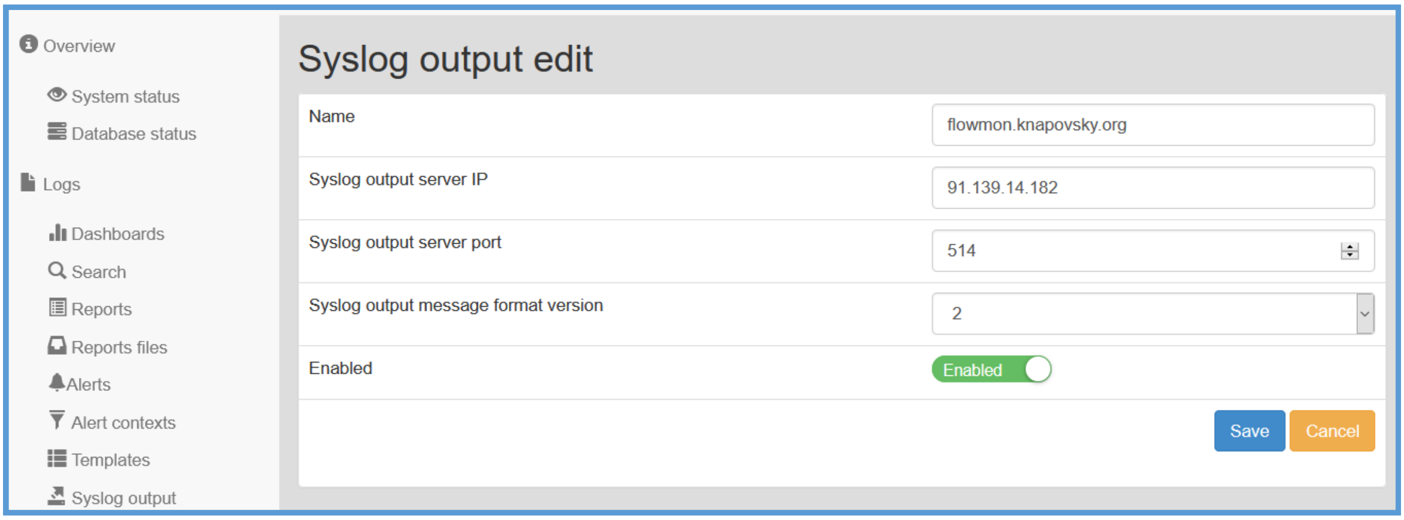
Policy	Setting
Audit Kerberos Authentication Service	Success

Policy	Setting
Audit Logon	Success

No settings defined.

Figure: preview of the result of creating a new audit policy in the MS AD

2. **LOGmanager configuration:** First you need to define a new destination for sending selected logs to the Flowmon syslog collector. In the LOGmanager menu *Logs / Syslog output,* it is necessary to add a new redirection. Fill in the form with the IP address and port (the default port for syslog is 514), where Flowmon listens, in *the Syslog output message format version* field, set the value to **2** and check the *Enabled* option. Save the configuration with the *Save* button. Below you can find a screenshot of the newly created record.

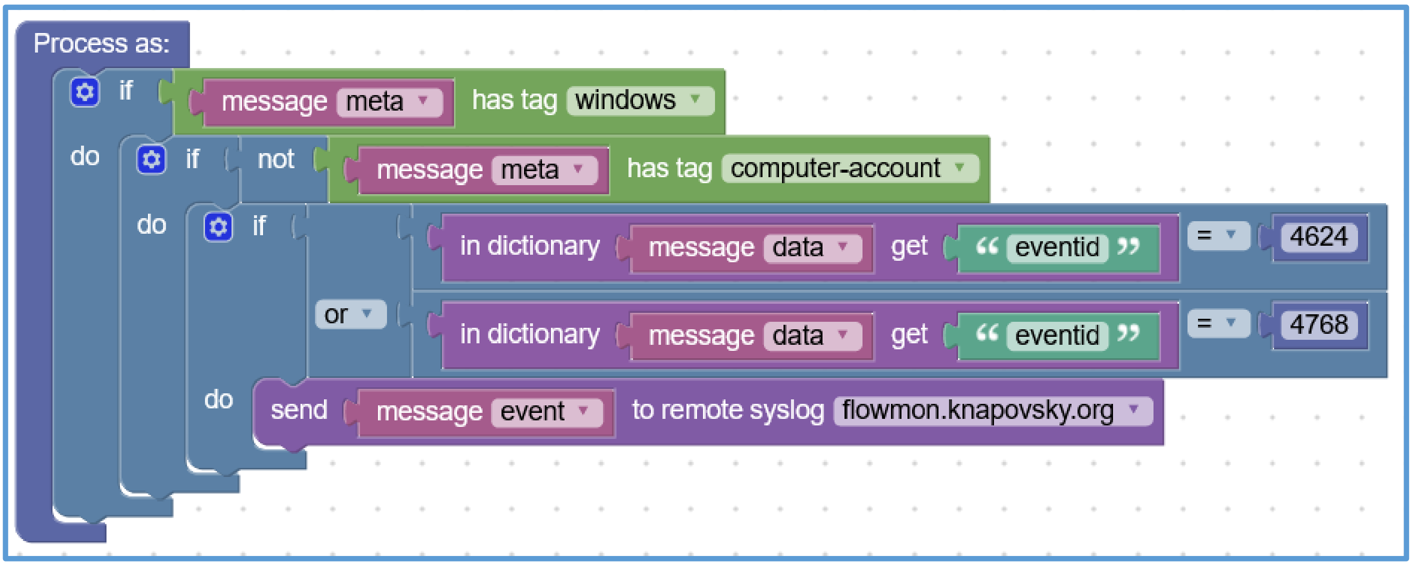


Syslog output edit

Name	flowmon.knapovsky.org
Syslog output server IP	91.139.14.182
Syslog output server port	514
Syslog output message format version	2
Enabled	Enabled

Figure: preview of creating a new destination for sending logs

3. Next, you need to create an alert according to the example below, which will forward the selected audit events to Flowmon. In the menu *Logs / Alerts* add a new alert. In the form for a new notification it is necessary to fill in the name or description, in the destination field fill in the e-mail address and check the *Enabled* option. In the Blocks field, create an alert as shown below. In the “send to remote syslog” block, select the redirection created in the previous step. Finally, save the configuration with the Save button.



```
Process as:
  if  message meta has tag windows
  do  if not message meta has tag computer-account
      do  if  in dictionary message data get “eventid” = 4624
              or
              in dictionary message data get “eventid” = 4768
          do  send message event to remote syslog flowmon.knapovsky.org
```

Figure: Preview of creating a action block for sending desired logs to Flowmon

4. **Flowmon configuration:** In Flowmon Configuration centre / System a new Syslog server must be added on the System Settings tab. The Enable external syslog protocols option must be selected and the New Syslog Client button must be used to set the information from which events will come. In this case, there will be the IP address of the LOGmanager system, port 514 (this is the same port that is set in the forwarding configuration in LOGmanager) and the TCP protocol. Next, you need to turn on the Enable parsing of user identity information option and create two new parsing rules using the New rule button to retrieve information from events 4624 and 4768.

   In the first new rule for event 4624, enter a suitable name in the *Name* field (for example, Windows Logon 4624) and enter the following rule in the *Log message rule* field:

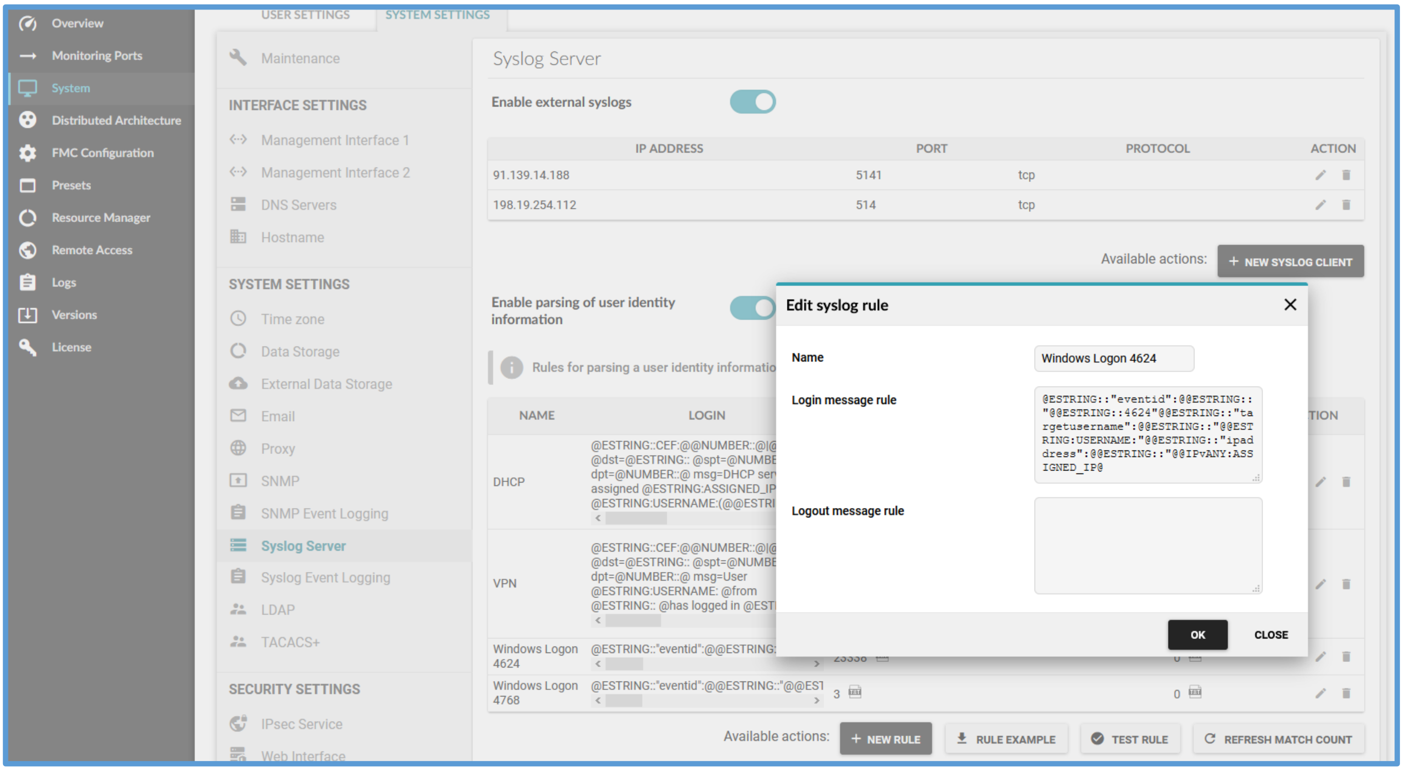
   ```
   @ESTRING::"eventid":@@ESTRING::"@@ESTRING::4624"@@ESTRING::"targetusername":@
   @ESTRING::"@@ESTRING:USERNAME:"@@ESTRING::"ipaddress":@@ESTRING::"@@IPvANY:AS
   SIGNED_IP@
   ```

   In the second new rule for event 4768, enter another suitable name in the *Name* field (for example, Windows Logon 4768) and enter the following rule in the *Log message rule* field:

   ```
   @ESTRING::"eventid":@@ESTRING::"@@ESTRING::4768"@@ESTRING::"targetusername":@
   @ESTRING::"@@ESTRING:USERNAME:"@@ESTRING::"ipaddress":@@ESTRING::"::ffff:@@IP
   vANY:ASSIGNED_IP@
   ```

   Finally, you need to press the *Save* button to save the configuration.

   An screenshot of the example of the newly created parsing rule record can be found below.



Syslog Server

Enable external syslogs

IP ADDRESS	PORT	PROTOCOL	ACTION
91.139.14.188	5141	tcp	
198.19.254.112	514	tcp	

Available actions:

Enable parsing of user identity information

Rules for parsing a user identity informatio

NAME	LOGIN			TION
DHCP	@ESTRING::CEF:@@NUMBER::@|@ @dst=@ESTRING:: @spt=@NUMBE dpt=@NUMBER::@ msg=DHCP ser assigned @ESTRING:ASSIGNED_IP @ESTRING:USERNAME:(@@ESTRI			
VPN	@ESTRING::CEF:@@NUMBER::@|@ @dst=@ESTRING:: @spt=@NUMBE dpt=@NUMBER::@ msg=User @ESTRING:USERNAME: @from @ESTRING:: @has logged in @ESTI			
Windows Logon 4624	@ESTRING::"eventid":@@ESTRING:	23338	0	
Windows Logon 4768	@ESTRING::"eventid":@@ESTRING::"@@EST	3	0	

Available actions:

Edit syslog rule

Name: Windows Logon 4624

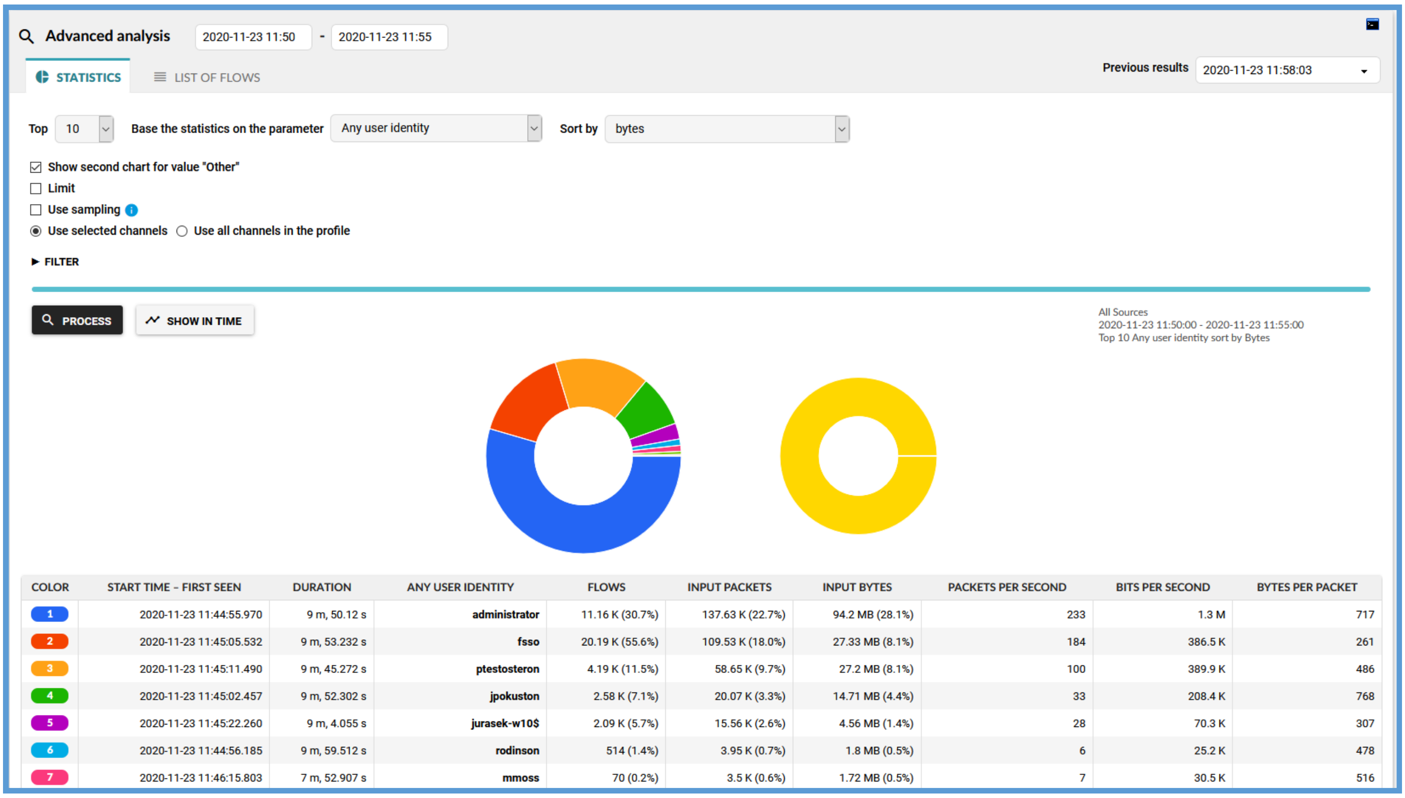
Login message rule:

```
@ESTRING::"eventid":@@ESTRING::
"@@ESTRING::4624"@@ESTRING::"ta
rgetusername":@@ESTRING::"@@EST
RING:USERNAME:"@@ESTRING::"ipad
dress":@@ESTRING::"@@IPvANY:ASS
IGNED_IP@
```

Logout message rule:

Figure: Preview of creating a new syslog rule in Flowmon

5. **Functionality verification:** The correct integration of user identity processing can be verified, for example, in the *Monitoring Centre*. In the menu, select *Analysis*, and at the bottom of the *Advanced Analysis* page, select *User Identity* in the *Base Statistics on the parameter*. Then click the *Process* button. If everything is correct, the statistics of data flows according to the identity of the users will be displayed as in the screenshot below.



2020-11-23 11:50 - 2020-11-23 11:55

Previous results 2020-11-23 11:58:03

Top 10 Base the statistics on the parameter Any user identity Sort by bytes

☑ Show second chart for value "Other"
☐ Limit
☐ Use sampling
● Use selected channels ○ Use all channels in the profile

All Sources
2020-11-23 11:50:00 - 2020-11-23 11:55:00
Top 10 Any user identity sort by Bytes

COLOR	START TIME – FIRST SEEN	DURATION	ANY USER IDENTITY	FLOWS	INPUT PACKETS	INPUT BYTES	PACKETS PER SECOND	BITS PER SECOND	BYTES PER PACKET
1	2020-11-23 11:44:55.970	9 m, 50.12 s	**administrator**	11.16 K (30.7%)	137.63 K (22.7%)	94.2 MB (28.1%)	233	1.3 M	717
2	2020-11-23 11:45:05.532	9 m, 53.232 s	**fsso**	20.19 K (55.6%)	109.53 K (18.0%)	27.33 MB (8.1%)	184	386.5 K	261
3	2020-11-23 11:45:11.490	9 m, 45.272 s	**ptestosteron**	4.19 K (11.5%)	58.65 K (9.7%)	27.2 MB (8.1%)	100	389.9 K	486
4	2020-11-23 11:45:02.457	9 m, 52.302 s	**jpokuston**	2.58 K (7.1%)	20.07 K (3.3%)	14.71 MB (4.4%)	33	208.4 K	768
5	2020-11-23 11:45:22.260	9 m, 4.055 s	**jurasek-w10$**	2.09 K (5.7%)	15.56 K (2.6%)	4.56 MB (1.4%)	28	70.3 K	307
6	2020-11-23 11:44:56.185	9 m, 59.512 s	**rodinson**	514 (1.4%)	3.95 K (0.7%)	1.8 MB (0.5%)	6	25.2 K	478
7	2020-11-23 11:46:15.803	7 m, 52.907 s	**mmoss**	70 (0.2%)	3.5 K (0.6%)	1.72 MB (0.5%)	7	30.5 K	516

Please, provide feedback and suggestions on this guide to: security-team@logmanager.com.

ABOUT THE MANUFACTURER

LOGmanager has been developed since 2014 as a flagship product of Sirwisa a.s., a company based in Prague. You can find selected customer references at www.logmanager.com. Our customers include not only government authorities, but also businesses of all sizes from all sectors, business corporations, banking organizations and more. Do not hesitate to contact us for more detailed customer references directly from your area of business. We will be happy to provide contacts to existing customers, who have agreed to be included on our list of references.