opFlow 3.0 API Reference

Authentication

Authentication is required to access all methods listed below.

POST login (authenticate)

`POST /en/omk/opFlow/login`

Authenticate to opFlow.

Request

Parameter	Description
username	The username to authenticate with
password	The password for the user

Successful Response

A cookie is created and sent with the response. This must be saved and passed with all requests below.

Obtaining data from the API

Get Request, submitting the parameters required on the table below.

`GET /en/omk/opFlow/data_model_view/new.json?requestData={"parameters":{}}`

Common Parameters and Required Parameters

Many of the parameters are common over all calls and are used when they make sense.

Some parameters are required and marked with a font wight: **bold**.

Parameters

Parameter	Description
start_date_raw	Epoch time to start the time period.
end_date_raw	Epoch time to end the time period.
group_by	Accepts a List of values. Values: "application", "src_ip", "dst_ip",etc. e.g: To group by "Application Conversations" ***"group_by":["src_ip","dst_ip","application"]*** *Note: This parameter is required and needs at least to be set to one value to work.*

<table>
<tr><td>flow_type</td><td>Accepts a list of values, is used to specify the summary type.
<table><tr><th>Summary type</th><th>Value</th></tr><tr><td>App Sources</td><td>["src_ip","application"]</td></tr><tr><td>App Destinations</td><td>["dst_ip","application"]</td></tr><tr><td>Applications</td><td>["application"]</td></tr><tr><td>TOS</td><td>[“tos”]</td></tr><tr><td>Talkers</td><td>["src_ip"]</td></tr><tr><td>Listeners</td><td>["dst_ip"]</td></tr></table></td></tr>
<tr><td>options</td><td>Is a has and accepts the following parameters:
<table><tr><th>Parameter</th><th>Possible value</th></tr><tr><td>limit</td><td>number of rows to return</td></tr><tr><td>sort:</td><td>Accepts a Hash of values
e.g: {"octets":-1}</td></tr><tr><td>only_reply_data</td><td>Set to true to only receive the reply data, if set to false, the request data will be also returned.</td></tr></table></td></tr>
</table>

Parameter	Description
model	The model used to obtain the flow summaries. Value must be set to: **"opFlow_flows_summary"**

Model view

Parameter	Description
model_view	Set value to: "**raw**" Return the data in JSON format.

Search

It is possible to do a search with the following argument passed to the request.

argument	options
&search={ }	Accepts a hash of values, but only one can be use at a time.
	Possible values to search by "Applications", "Source", "Source Port", "Destination" and "Destination Port" "application":"regex:**abc**" "dnsname_src_ip":"regex:**abc**" "src_port":"portNumber" "dnsname_dst_ip":"regex:**abc**" "dnsname_dst_ip":"regex:**abc**" "dst_port":"portNumber" Where **abc** is a string or text to search for.

TopN

Required Parameters (along with common parameters)

To obtain TopN data. The TopN limit must be set in the option list.

Parameter	Description
options	Is a has and accepts the following parameters: **Parameter** / **Possible value** limit / number of rows to return

Request example output:

Get Top 5 Applications from October 10. 2018 4:22:00 PM GMT+10:00 (1539152520) to October 10, 2018 6:22:00 PM GMT+10:00 (1539159720), sorted by octets (bytes) in descending order, getting only reply data.

```
http://demo.opmantek.com/en/omk/opFlow/data_model_view/new.json?requestData={"parameters":{"start_date_raw":1539152520,"end_date_raw":1539159720,"group_by":["application"],"flow_type":["application"]},"options":{"limit":5,"sort":{"octets":-1},"only_reply_data":"true"},"model":"opFlow_flows_summary","model_view":"raw"}
```

Response

```
[{
                "application": "UDP:32760",
                "avg_octets_sec": null,
                "avg_packets_sec": null,
                "duration": 28642.8639996052,
                "flows": 628,
                "flows_pct": 0.00888348209865192,
                "octets": 440351659,
                "octets_pct": 0.814896754348869,
                "packets": 769974,
                "packets_pct": 0.592798410938655
        },
        {
                "application": "snmp",
                "avg_octets_sec": null,
                "avg_packets_sec": null,
                "duration": 31849.9360135078,
                "flows": 7227,
                "flows_pct": 0.102230772495155,
                "octets": 58955621,
                "octets_pct": 0.109100858874071,
                "packets": 302235,
                "packets_pct": 0.232688932002956
        },
        {
                "application": "https",
                "avg_octets_sec": null,
                "avg_packets_sec": null,
                "duration": 32292.7479987144,
                "flows": 4369,
                "flows_pct": 0.0618024415430099,
                "octets": 24644811,
                "octets_pct": 0.0456066784011851,
                "packets": 46621,
                "packets_pct": 0.0358932310914018
        },
        {
                "application": "ICMP:Echo Request",
                "avg_octets_sec": null,
                "avg_packets_sec": null,
                "duration": 542978.315999269,
                "flows": 26946,
                "flows_pct": 0.381169281258399,
                "octets": 7545636,
                "octets_pct": 0.0139636451009669,
                "packets": 89845,
                "packets_pct": 0.0691711320522296
        },
        {
                "application": "ICMP:Echo Reply",
                "avg_octets_sec": null,
                "avg_packets_sec": null,
                "duration": 335198.47600317,
                "flows": 11506,
                "flows_pct": 0.16276010354632,
                "octets": 3207540,
                "octets_pct": 0.00593574222334012,
                "packets": 38201,
                "packets_pct": 0.0294107230845036
        }
]
```