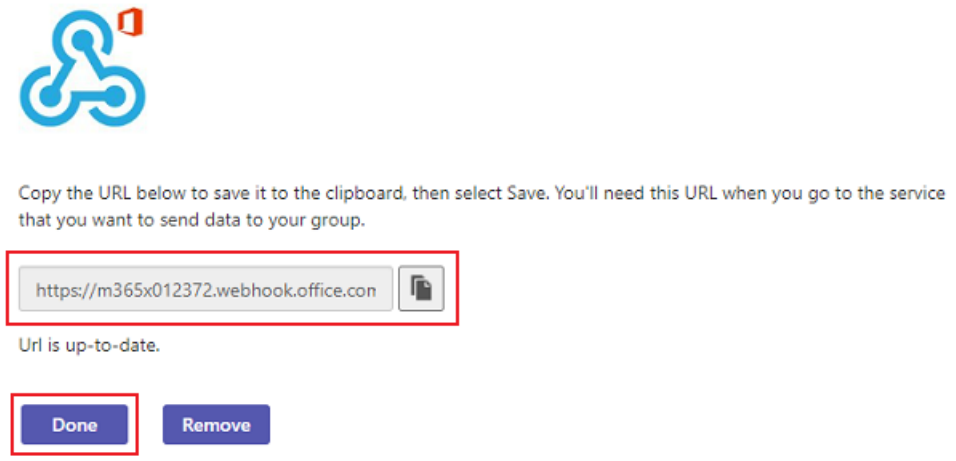
Flowmon ADS Integration with Teams

Microsoft Teams Incoming Webhook Script Usage

Teams Configuration

Configuration of the Incoming webhook is described at https://learn.microsoft.com/en-us/microsoftteams/platform/webhooks-and-connectors/how-to/add-incoming-webhook

You only need to select a group and add connector there. This webhook will provide you with HTTPs URL where the script will send (POST) the messages.



There is a limitation on how many messages could be sent through the webhook. The details are available at https://learn.microsoft.com/en-us/microsoftteams/platform/webhooks-and-connectors/how-to/connectors-using

Current numbers are four messages in a second and sixty in 30 seconds and 100 in five minutes. So, this should be deployed really only on the important event or well configured Flowmon ADS system.

Flowmon ADS Configuration

Details on how to configure a custom script are in the User Guide section 2.3.18 of the Flowmon ADS.

You have two options to provide the parameters in the script itself before uploading.

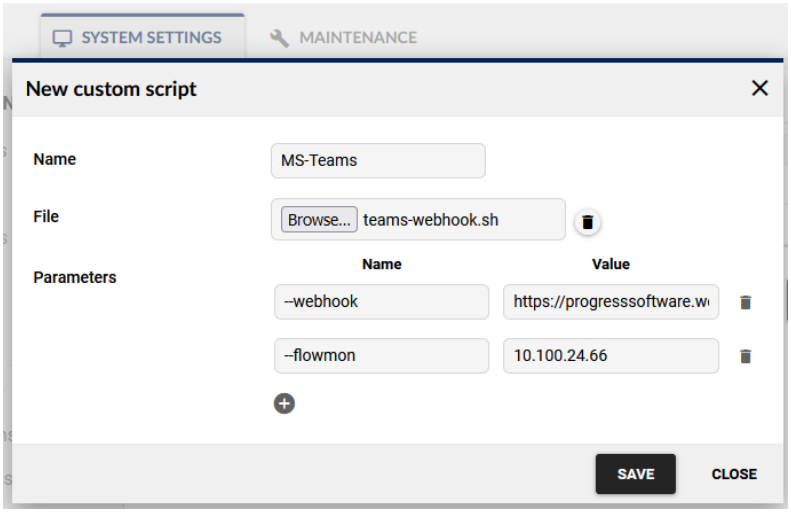
```
# Debug 1 = yes, 0 = no
DEBUG=1
TEST=0
# Incoming webhook URL
WEBHOOK='https://progresssoftware.webhook.office.com/webhookb2/4b
# hostname / IP of Flowmon Web UI for links in the messages
FLOWMON='10.100.24.66'
```

Or to provide these by parameters when after uploading and specifying the URL and your Flowmon web UI hostname or IP address.

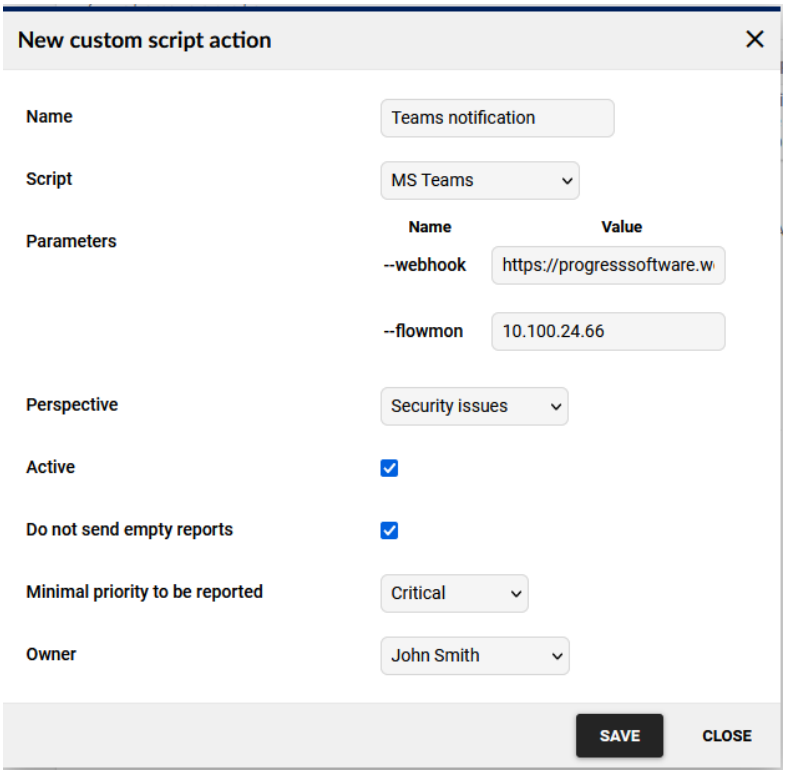
```
usage: teams-webhook.sh <options>
Optional:

--webhook   MS Teams Webhook
--flowmon   IP / Hostname of Flowmon Web UI for links
--test      This will send a test message with static text
```

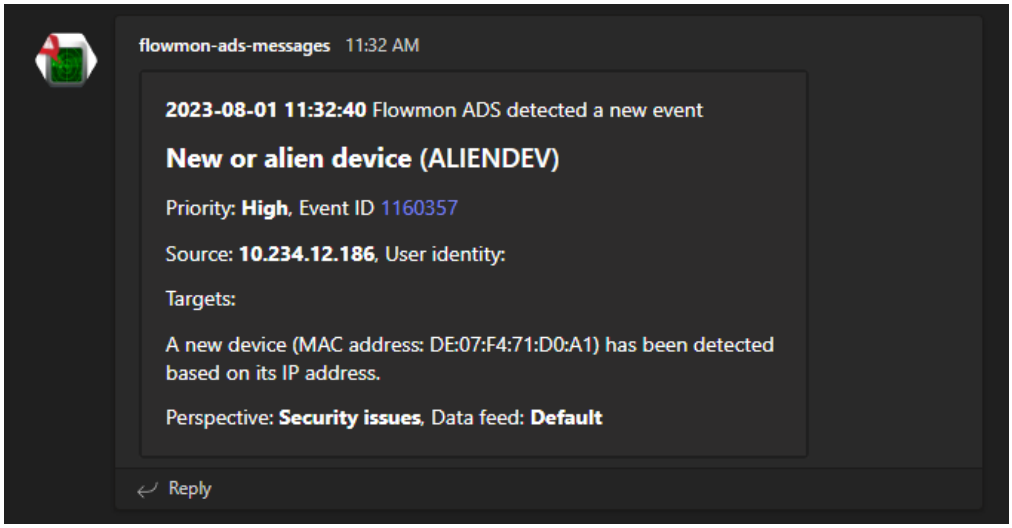
For example, we can create a custom script with those parametres to be different from default.



And then configure action where it will allow you to change the parameters.



You can also test if from any Linux machine when you use parameter test with some value after it. The output in teams would looks like on image below.


flowmon-ads-messages 11:32 AM
2023-08-01 11:32:40 Flowmon ADS detected a new event
New or alien device (ALIENDEV)
Priority: High, Event ID 1160357
Source: 10.234.12.186, User identity:
Targets:
A new device (MAC address: DE:07:F4:71:D0:A1) has been detected based on its IP address.
Perspective: Security issues, Data feed: Default
Reply