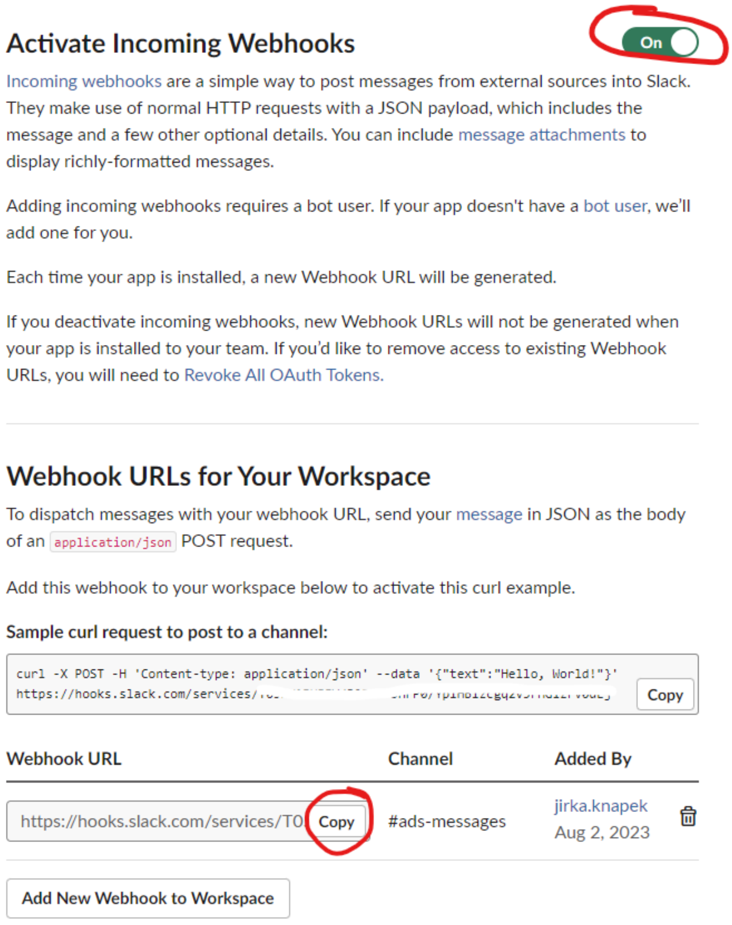
Flowmon ADS Integration with Slack

Slack Webhook Script Usage

Slack Configuration

Configuration of the Incoming webhook is described at https://api.slack.com/messaging/webhooks

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



Activate Incoming Webhooks

Incoming webhooks are a simple way to post messages from external sources into Slack. They make use of normal HTTP requests with a JSON payload, which includes the message and a few other optional details. You can include message attachments to display richly-formatted messages.

Adding incoming webhooks requires a bot user. If your app doesn't have a bot user, we'll add one for you.

Each time your app is installed, a new Webhook URL will be generated.

If you deactivate incoming webhooks, new Webhook URLs will not be generated when your app is installed to your team. If you'd like to remove access to existing Webhook URLs, you will need to Revoke All OAuth Tokens.

Webhook URLs for Your Workspace

To dispatch messages with your webhook URL, send your message in JSON as the body of an `application/json` POST request.

Add this webhook to your workspace below to activate this curl example.

Sample curl request to post to a channel:

```
curl -X POST -H 'Content-type: application/json' --data '{"text":"Hello, World!"}'
https://hooks.slack.com/services/[redacted]
```

Webhook URL	Channel	Added By
https://hooks.slack.com/services/T0	#ads-messages	jirka.knapek Aug 2, 2023

There is a limitation on how many messages could be sent through the webhook. The current limit is a message in one second. So, this should be deployed really only on the important event or well configured Flowmon ADS system.

Flowmon ADS Configuration

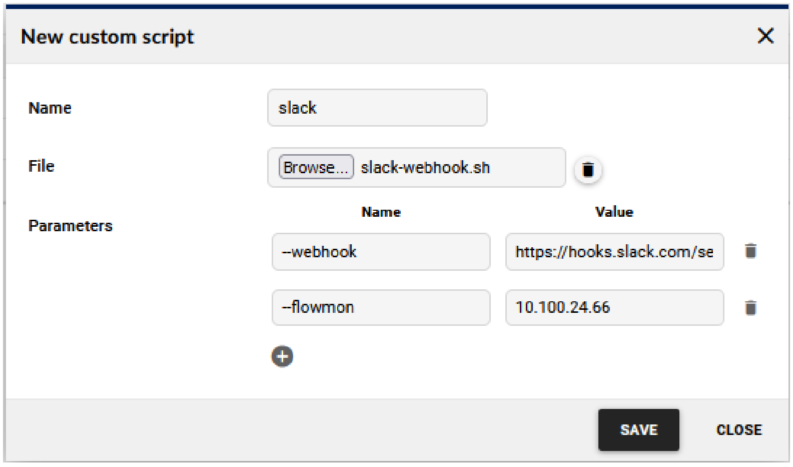
Details on how to configure a custom script are in the User Guide section 2.3.18 of the Flowmon ADS.

You have two options to provide the parameters in the script itself before uploading or to provide these by parameters when after uploading and specifying the URL and your Flowmon web UI hostname or IP address.

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

--webhook    slack 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 parameters to be different from default.



New custom script

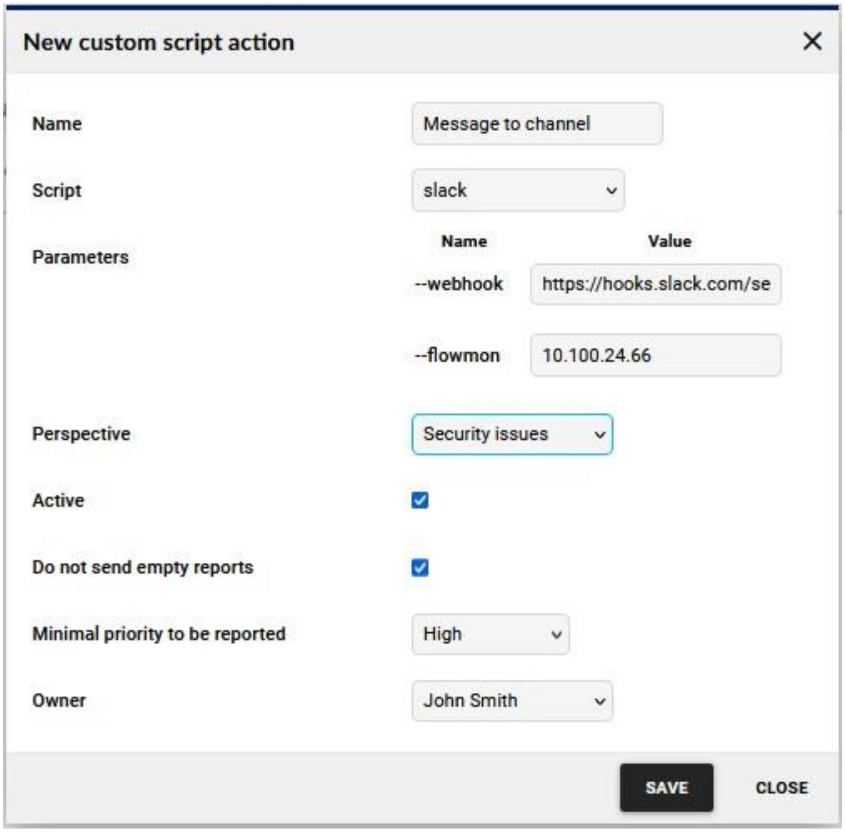
Name: slack

File: Browse... slack-webhook.sh

Parameters:

Name	Value
--webhook	https://hooks.slack.com/se
--flowmon	10.100.24.66

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



New custom script action

Name: Message to channel

Script: slack

Parameters:

Name	Value
--webhook	https://hooks.slack.com/se
--flowmon	10.100.24.66

Perspective: Security issues

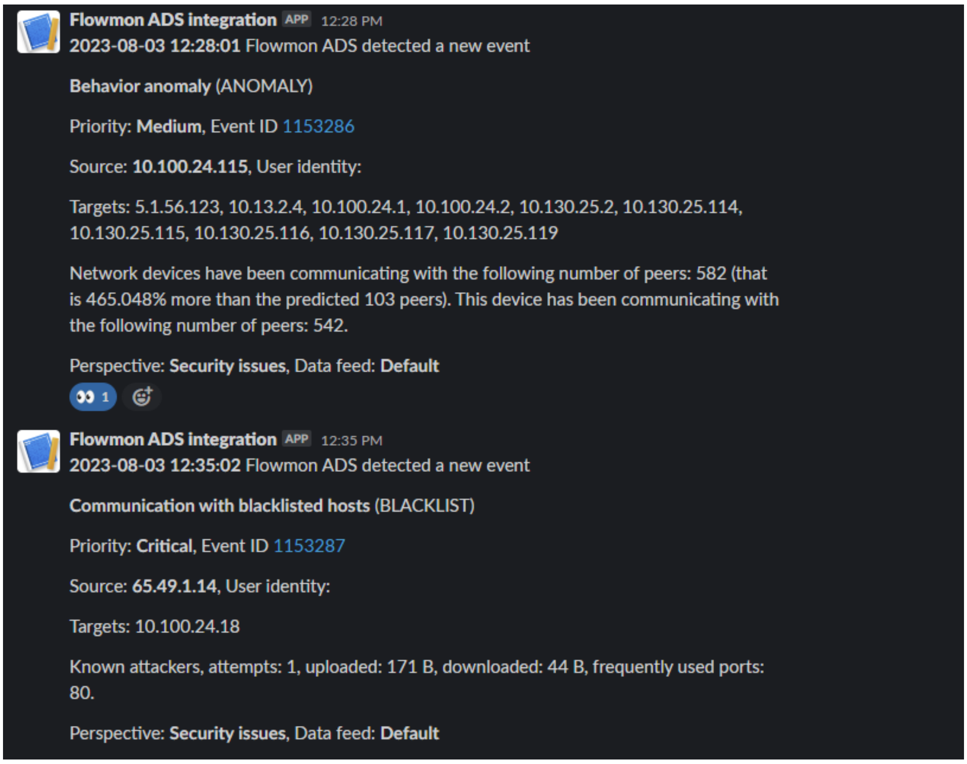
Active: ☑

Do not send empty reports: ☑

Minimal priority to be reported: High

Owner: John Smith

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.



2023-08-03 12:28:01 Flowmon ADS detected a new event

Behavior anomaly (ANOMALY)

Priority: **Medium**, Event ID 1153286

Source: **10.100.24.115**, User identity:

Targets: 5.1.56.123, 10.13.2.4, 10.100.24.1, 10.100.24.2, 10.130.25.2, 10.130.25.114, 10.130.25.115, 10.130.25.116, 10.130.25.117, 10.130.25.119

Network devices have been communicating with the following number of peers: 582 (that is 465.048% more than the predicted 103 peers). This device has been communicating with the following number of peers: 542.

Perspective: **Security issues**, Data feed: **Default**

2023-08-03 12:35:02 Flowmon ADS detected a new event

Communication with blacklisted hosts (BLACKLIST)

Priority: **Critical**, Event ID 1153287

Source: **65.49.1.14**, User identity:

Targets: 10.100.24.18

Known attackers, attempts: 1, uploaded: 171 B, downloaded: 44 B, frequently used ports: 80.

Perspective: **Security issues**, Data feed: **Default**