


# Falco Slack Notifications

Go to <https://api.slack.com/apps>

Select incoming webhooks

 falco app

Settings

Basic Information

Collaborators

Socket Mode

Install App

Manage Distribution

Features

App Home

Org Level Apps

Incoming Webhooks

Interactivity & Shortcuts

Slash Commands

Workflow Steps

OAuth & Permissions

Event Subscriptions

User ID Translation


App Manifest NEW

Beta Features

Submit to App Directory

Review & Submit

Give feedback

Slack 

Help

Contact

Policies

Our Blog

## Incoming Webhooks

### Activate Incoming Webhooks

On

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!"}'  
YOUR_WEBHOOK_URL_HERE
```

Webhook URL	Channel	Added By
No webhooks have been added yet.		

Add New Webhook to Workspace

Select add new webhook to workspace



## falco app is requesting permission to access the devsecops Slack workspace

### Where should falco app post?

# falco app requires a channel to post to as an app

Cancel

Allow

Select channel and allow

## 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]
```

Copy

### Webhook URL

### Channel

### Added By

[https://hooks.slack.com/services/\[REDACTED\]](https://hooks.slack.com/services/[REDACTED])

Copy

#falco

dai

Apr 14, 2023



Add New Webhook to Workspace

We can copy sample curl to test connection and update webhook-url into falco.

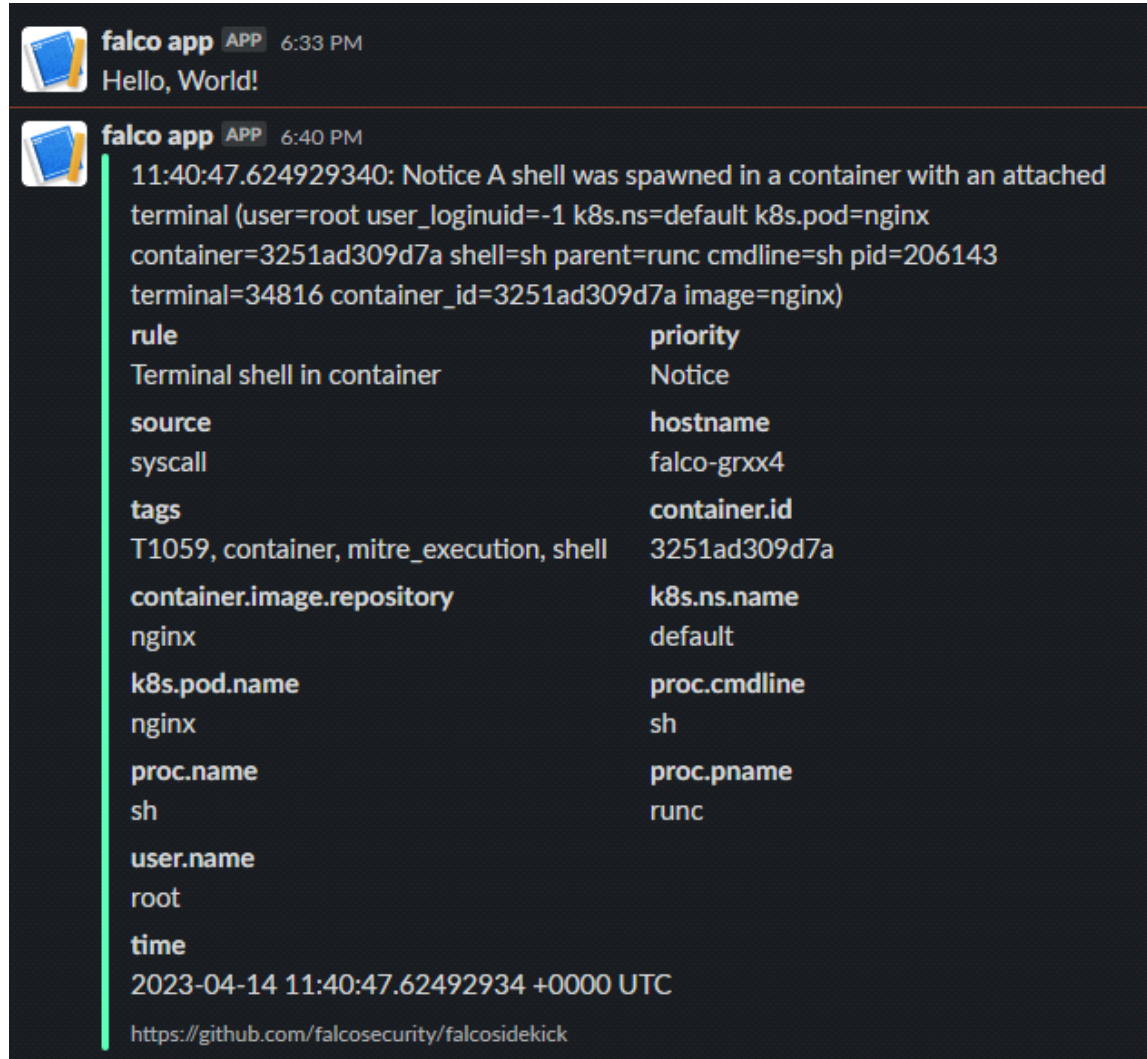
```
helm upgrade falco falcosecurity/falco \  
--set falcosidekick.enabled=true \  
--set falcosidekick.webui.enabled=true \  

```

```
--set falcosidekick.config.slack.webhookurl="https://hooks.slack.com/services/<ID>" \
-n falco
```

Execute shell nginx to test notification:

```
kubectl exec -it nginx -- sh
```



The screenshot shows a Slack interface with a message from 'falco app' at 6:33 PM saying 'Hello, World!'. Below it, another message from 'falco app' at 6:40 PM displays a detailed notification. The notification text is as follows:

11:40:47.624929340: Notice A shell was spawned in a container with an attached terminal (user=root user\_loginuid=-1 k8s.ns=default k8s.pod=nginx container=3251ad309d7a shell=sh parent=runc cmdline=sh pid=206143 terminal=34816 container\_id=3251ad309d7a image=nginx)

rule	priority
Terminal shell in container	Notice

source	hostname
syscall	falco-grxx4

tags	container.id
T1059, container, mitre_execution, shell	3251ad309d7a

container.image.repository	k8s.ns.name
nginx	default

k8s.pod.name	proc.cmdline
nginx	sh

proc.name	proc.pname
sh	runc

user.name
root

**time**  
2023-04-14 11:40:47.62492934 +0000 UTC

<https://github.com/falcosecurity/falcosidekick>