GitHub getting started guide

Version 2.0

February 7, 2020

www.expel.io

What's in this guide?

Howdy! In this guide, you'll find instructions on how to:

1. Generate the Application Program Interface (API) Credentials; and
2. Configure the GitHub in Expel Workbench™.

Step 1 — Generate API credentials

The GitHub integration polls events from the GraphQL API and only a Personal Access Token is required.

A. A Personal Access Token can be created by navigating to your **Account Settings** via the menu under your profile photo in the top-right of any page.

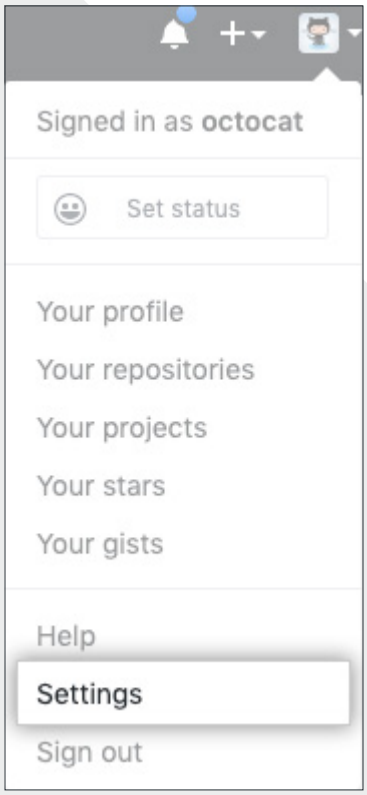

Figure 1

B. In the left sidebar, click **Developer settings**

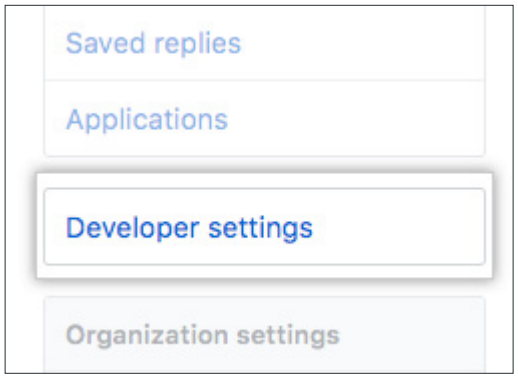

Figure 2

C. In the left sidebar, click **Personal access tokens**

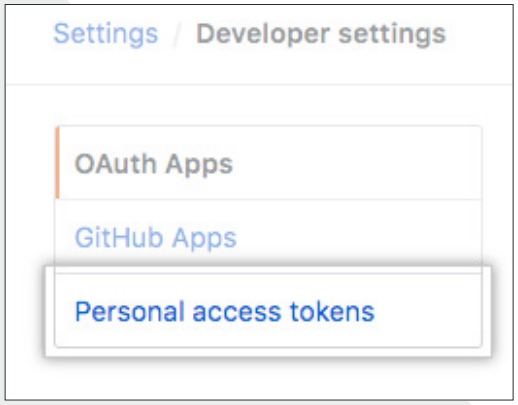

Figure 3

D. Click **Generate new token**

Figure 4

E. Please grant the token the defined permissions from the image below

Figure 5

F. Generate the token

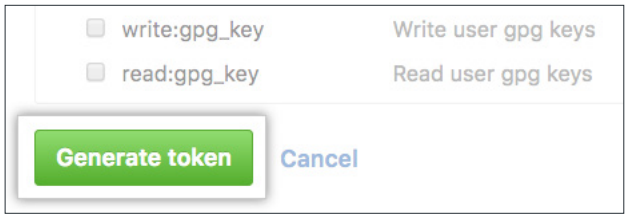

Figure 6

G. Enable SSO if the option is available

Figure 7

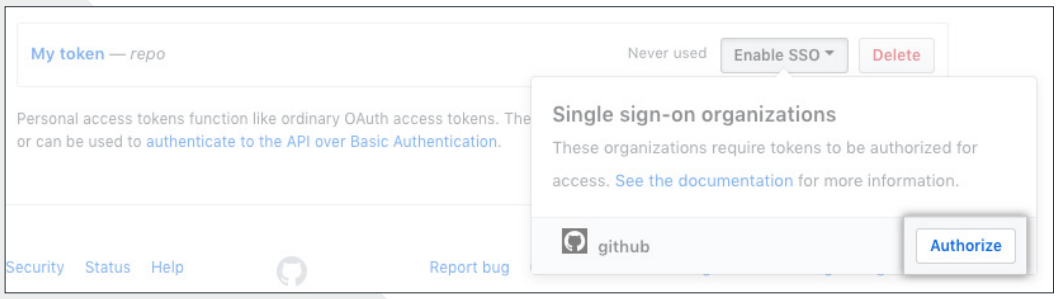

Figure 8

H. Click to copy the token to your clipboard. For security reasons, after you navigate off the page, you will not be able to see the token again

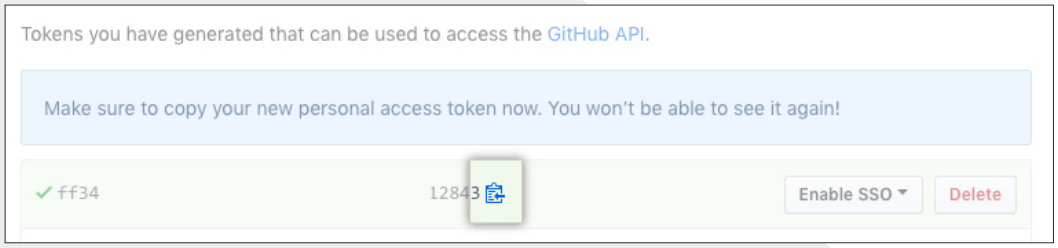

Figure 9

I. Please use this token when configuring GitHub in Workbench

Step 2 — Configure the technology in Workbench

Now that we have all the correct access configured and have noted the credentials, we can integrate GitHub with Expel Workbench.

Register device in Expel Workbench

A. In a new browser tab, login to https://workbench.expel.io

B. Enter Security Code from Google Authenticator (two-factor authentication)

C. On the console page, navigate to **Settings** and click **Security Devices**

D. At the top right of the page, select **Add Security Device** (Figure 10)

Figure 10

E. Search for and select your technology (GitHub)

F. For **SIEM** select Expel Cloud Service

G. Complete all fields using the credentials and information you collected in *Step 1* above

H. For **Name** enter the name of your GitHub organization

I. For **Location** enter “Cloud”

J. For **API key** enter the API generated in Step 1

K. For **Organization name**, enter the name of your GitHub organization

L. Select **Save**

Figure 11

M. After a few minutes (1–10 minutes), refresh the **Security Devices** page and you should see your device status reporting as *Healthy*, or if there is an issue, it will provide more details of what the issue may be

N. To check and see if alerts are coming through, navigate to **Alerts** on the console page. Click the icon in the upper right to switch to grid view, then check the list for GitHub alerts

That's it! Give yourself a pat on the back — you're done!

If you have any issues, concerns, questions or feedback,
please don't hesitate to contact Expel at devicehealth@expel.io.