



# GitHub getting started guide

Version 2.0

February 7, 2020

## 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.

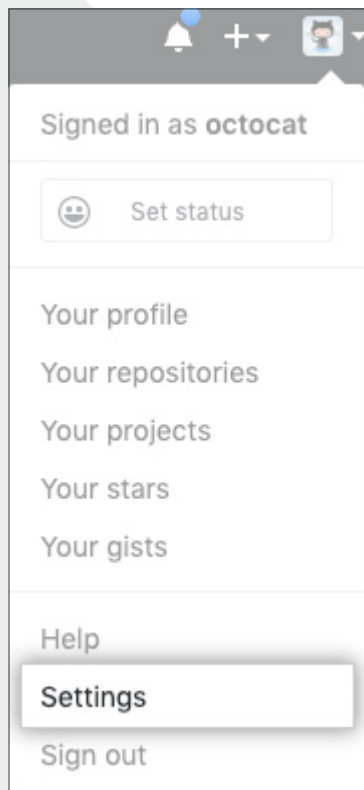


Figure 1

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

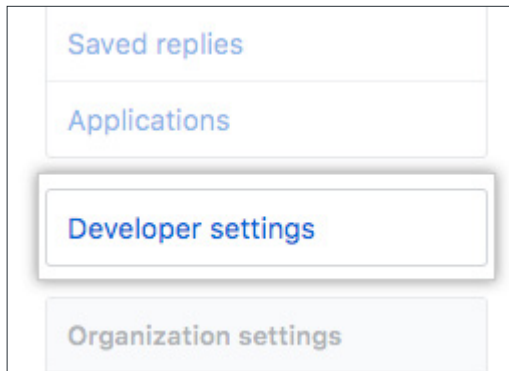


Figure 2

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

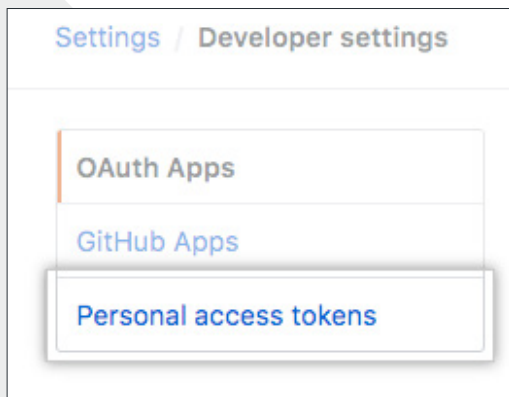


Figure 3

D. Click **Generate new token**

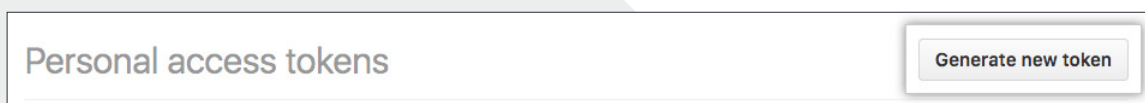


Figure 4

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

**Select scopes**

Scopes define the access for personal tokens. [Read more about OAuth scopes.](#)

<input checked="" type="checkbox"/> <b>repo</b>	Full control of private repositories
<input checked="" type="checkbox"/> repo:status	Access commit status
<input checked="" type="checkbox"/> repo_deployment	Access deployment status
<input checked="" type="checkbox"/> public_repo	Access public repositories
<input checked="" type="checkbox"/> repo:invite	Access repository invitations
<input checked="" type="checkbox"/> security_events	Read and write security events
<input type="checkbox"/> <b>workflow</b>	Update github action workflows
<input type="checkbox"/> <b>write:packages</b>	Upload packages to github package registry
<input type="checkbox"/> read:packages	Download packages from github package registry
<input type="checkbox"/> <b>delete:packages</b>	Delete packages from github package registry
<input checked="" type="checkbox"/> <b>admin:org</b>	Full control of orgs and teams, read and write org projects
<input checked="" type="checkbox"/> write:org	Read and write org and team membership, read and write org projects
<input checked="" type="checkbox"/> read:org	Read org and team membership, read org projects
<input type="checkbox"/> <b>admin:public_key</b>	Full control of user public keys
<input type="checkbox"/> write:public_key	Write user public keys
<input type="checkbox"/> read:public_key	Read user public keys
<input type="checkbox"/> <b>admin:repo_hook</b>	Full control of repository hooks
<input type="checkbox"/> write:repo_hook	Write repository hooks
<input type="checkbox"/> read:repo_hook	Read repository hooks
<input type="checkbox"/> <b>admin:org_hook</b>	Full control of organization hooks
<input type="checkbox"/> <b>gist</b>	Create gists
<input type="checkbox"/> <b>notifications</b>	Access notifications
<input checked="" type="checkbox"/> <b>user</b>	Update all user data
<input checked="" type="checkbox"/> read:user	Read all user profile data
<input checked="" type="checkbox"/> user:email	Access user email addresses (read-only)
<input checked="" type="checkbox"/> user:follow	Follow and unfollow users
<input type="checkbox"/> <b>delete_repo</b>	Delete repositories
<input type="checkbox"/> <b>write:discussion</b>	Read and write team discussions
<input type="checkbox"/> read:discussion	Read team discussions
<input checked="" type="checkbox"/> <b>admin:enterprise</b>	Full control of enterprises
<input checked="" type="checkbox"/> manage_billing:enterprise	Read and write enterprise billing data
<input checked="" type="checkbox"/> read:enterprise	Read enterprise profile data
<input type="checkbox"/> <b>admin:gpg_key</b>	Full control of public user gpg keys ( <a href="#">Developer Preview</a> )
<input type="checkbox"/> write:gpg_key	Write public user gpg keys
<input type="checkbox"/> read:gpg_key	Read public user gpg keys

Figure 5

F. Generate the token

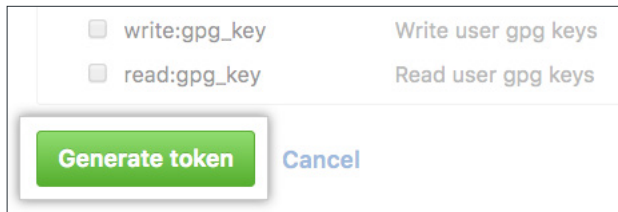


Figure 6

G. Enable SSO if the option is available

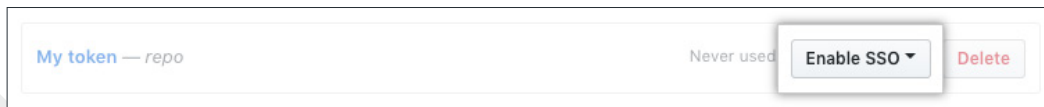


Figure 7

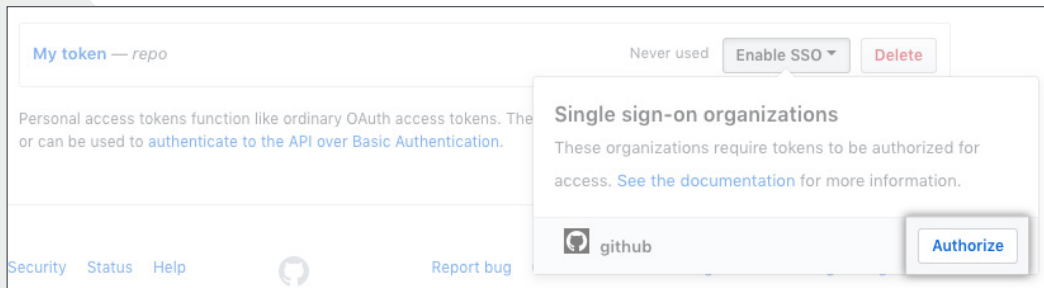


Figure 8

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

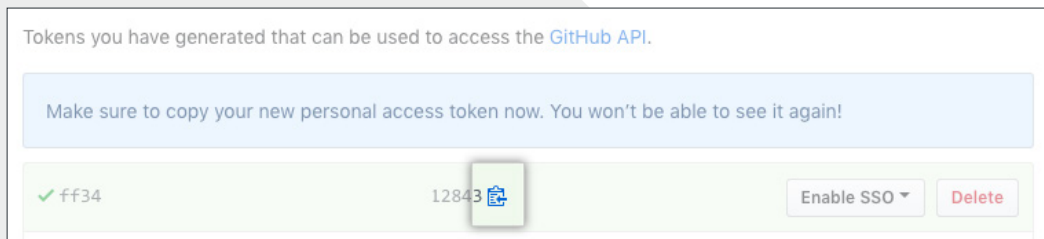


Figure 9

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**

The screenshot shows a web form titled "Add Security Device" with a search bar containing "Github" and a vendor dropdown set to "All vendors". The form is for a "GitHub" device. It includes the following fields:

- SIEM:** A dropdown menu with "Expel Cloud Service" selected.
- Name:** A text input field containing "GitHub-us".
- Location:** A text input field containing "Cloud".
- CONNECTION SETTINGS:**
  - API token:** A masked text input field with a "Show" link.
  - Organization name:** A text input field containing "expel-io".
- CONSOLE LOGIN (OPTIONAL):**
  - Console URL:** An empty text input field.
  - Username:** An empty text input field.
  - Password:** A masked text input field with a "Show" link.
  - Two-factor secret key (32-character code):** An empty text input field.

At the bottom right of the form are "Cancel" and "Save" buttons.

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](mailto:devicehealth@expel.io).