PLURALSIGHT | HELP CENTER

GitHub Enterprise Server setup

Tags: Flow

This is a step-by-step guide for connecting your GitHub Enterprise Server (self-hosted) account to Flow. If your repositories are behind a firewall, please allowlist our IPs on port 443 over HTTPS. You also need a public DNS record pointing to the IP address that is being exposed for Flow analysis. This DNS entry should match the TLS/SSL certificate the server is utilizing.

> **Important:** Use a service account to create this integration. Learn more about creating a service account.

In this article

Who can use this?

Core	Plus
✓	✓

Permission requirements

In order to utilize all integration services—including pull requests, tickets, and webhooks—the service account needs to be an owner on the GitHub organization.

If the service account is only a member of the organization, webhooks will not be available in Flow. All other services such as repos, PRs, and tickets will be available.

Webhook permissions

In order to enable Webhooks, the service account needs to be a GitHub organization owner and at least one repo needs to be imported from the organization. Learn more about webhooks.

OAuth Permissions

Flow only requires read access to your repositories. Flow needs this permission to process the metadata used to

generate our reports.

GitHub does not offer the ability to narrow permissions down to just read-only access to private profile information and repositories. When connecting to GitHub, their standard OAuth permissions include write and full admin permissions. These permissions are never used by our system. These access levels are required in order to utilize GitHub APIs.

back to top

Connecting to GitHub Enterprise Server

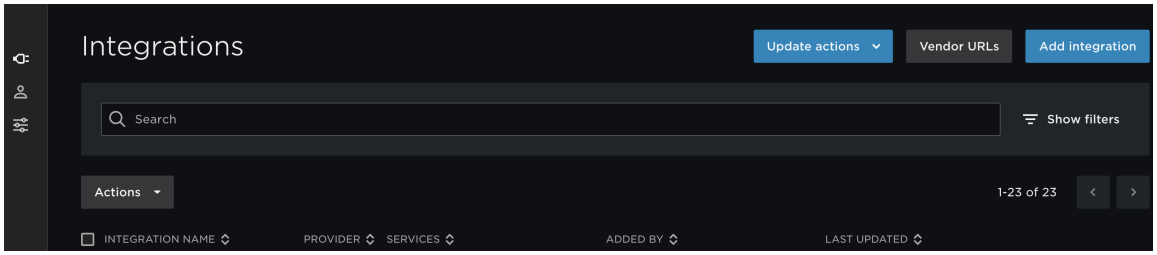
There are two ways you can connect to your GitHub Enterprise Server account:

1. OAuth requires you to create an OAuth application in your GitHub Enterprise Server account.
2. Access Token requires you to create an access token in your GitHub Enterprise Server account.

> **Note**: Before August 2020, Username/Password was a connection option. This option is no longer available. Integrations from before this date that used the Username/Password connection option will still work as long as the credentials aren't updated, but no new integrations can be created with this option.

To connect your GitHub Enterprise Server, first create a new integration.

1. In the top navigation, click **Settings.**
2. In the left navigation under **Integrations**, click **Integrations.**
3. Click **Add Integration** in the top right corner of the Integrations page.



4. Select **GitHub Enterprise Server (Self-hosted)** from the Integration Provider list and click **Next**.
5. Choose one of the three ways to connect your GitHub Enterprise Server account.

back to top

OAuth

Connecting via OAuth requires you to first create a new OAuth application (external site, opens in new tab) in your GitHub Enterprise account.

1. Create the OAuth application using the following information:

1. Create the OAuth application using the following information:
    - **Name:** Flow
    - **Homepage URL:** https://www.pluralsight.com
    - **Description:** Authorizing with your Flow account allows Flow to conveniently display your repos to make importing them efficient. You will get to pick which repos to import. Flow won't access any of your other repos.
    - **Callback URL:** https://flow.pluralsight.com/accounts/complete/github-enterprise/
2. Navigate back to the OAuth Apps page in your GitHub account. Gather the Client ID, Client Secret, and Base URL.
3. Paste this information into the authorization page in Flow.

    > **Tip:** Make sure you are not blocking pop-ups as you will need to authorize the application.

4. Click **Connect to GitHub Enterprise Server (Self-hosted)**.

If your connection was successful you will see a success message.

If you are not able to connect to your account, check your Client ID and Client Secret to make sure they are correct and try again.

To finish up your GitHub Enterprise Server integration, skip down to the Finishing up section below.

back to top

Access token

To connect via an access token, use the Access token authentication method. Create an access token in GitHub Enterprise Server (external site, opens in new tab).

1. In the Select Scopes section, select the scopes below. Flow needs these scopes in order to import and process your repos and projects and to enable webhooks.
    - repo (all)
    - admin:org
    - read:org
    - admin:repo_hook (all)
    - admin:org_hook
    - user
    - read:user
2. Once you have created your token, copy and paste it into your GitHub Enterprise Server integration in Flow and click **Test connection**.

If the connection was successful you will see a success message.

back to top

Finishing up

1. Once you have successfully connected to your GitHub Enterprise Server account, click **Next**.
2. On the next screen you will be selecting the services you want turned on for this integration. If you would like to import ticket and pull request data in addition to repo data, then leave all services on. You can turn services on and off at any time. Click **Next**.
3. Name your integration so you can identify the account you connected with. Click **Create**.
4. You have successfully created a new GitHub Enterprise Server integration.
5. To learn more about managing your new integration settings, see Manage integrations.

Troubleshooting

If you receive an error message when testing your connection during the setup process, check the following:

1. If we are unable to connect to your URL:
    1. Verify that Flow IP addresses are allowlisted if you are behind a firewall.
    2. Make sure your domain is accessible outside of your network with public DNS resolution. If your public domain is different from your internal domain, you will need a reverse proxy in place in order for Flow to be able to import and process your data.
    3. Make sure you're using a valid SSL certificate signed by a public CA.
2. If the authorization failed, check your credentials and try again.

If you need help, please contact Pluralsight Support.