Connecting with third-party applications

In this article

You can connect your GitHub Enterprise Server identity to third-party applications using OAuth. When authorizing one of these applications, you should ensure you trust the application, review who it's developed by, and review the kinds of information the application wants to access.

When a third-party application wants to identify you by your GitHub Enterprise Server login, you'll see a page with the developer contact information and a list of the specific data that's being requested.

Contacting the application developer

Because an application is developed by a third-party who isn't GitHub Enterprise Server, we don't know exactly how an application uses the data it's requesting access to. If you have questions or concerns about an application, you should contact the application developer. To find contact information for an application, you can click the account name of the developer at the top of of the app's authorization page.

If the developer has chosen to supply further information, the right-hand side of the authorization page may also provide a detailed description of the application, as well as its associated website.

Types of application access and data

Applications can have *read* or *write* access to your GitHub Enterprise Server data.

- **Read access** only allows an application to *look at* your data.
- **Write access** allows an application to *change* your data.

About OAuth scopes

Scopes are named groups of permissions that an application can request to access both public and non-public data.

When you want to use a third-party application that integrates with GitHub Enterprise Server, that application lets you know what type of access to your data will be required. If you grant access to the application, then the application will be able to perform actions on your behalf, such as reading or modifying data. For example, if you want to use an app that requests `user:email` scope, the app will have read-only access to your private email addresses. For more information, see "Scopes for OAuth apps."

Note: Currently, you can't scope source code access to read-only.

Tip: We recommend that you regularly review your authorized integrations. Remove any applications and tokens that haven't been used in a while. For more information, see "Reviewing your authorized OAuth apps."

Types of requested data

There are several types of data that applications can request.

Type of data	Description
Commit status	You can grant access for a third-party application to report your commit status. Commit status access allows applications to determine if a build is a successful against a specific commit. Applications won't have access to your code, but they *can* read and write status information against a specific commit.
Deployments	Deployment status access allows applications to determine if a deployment is successful against a specific commit for a repository. Applications won't have access to your code.
Gists	Gist access allows applications to read or write to both your public and secret Gists.
Hooks	Webhooks access allows applications to read or write hook configurations on repositories you manage.
Notifications	Notification access allows applications to read your GitHub Enterprise Server notifications, such as comments on issues and pull requests. However, applications remain unable to access anything in your repositories.
Organizations and teams	Organization and teams access allows apps to access and manage organization and team membership.
Personal user data	User data includes information found in your user profile, like your name, e-mail address, and location.
Repositories	Repository information includes the names of contributors, the branches you've created, and the actual files within your repository. An application can request access to all of your repositories of any visibility level. For more information, see "About repositories."
Repository delete	Applications can request to delete repositories that you administer, but they won't have access to your code.