Authorizing OAuth apps

In this article

You can connect your GitHub Enterprise Cloud identity to third-party applications using OAuth. When authorizing an OAuth app, 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 an OAuth app wants to identify you by your account on GitHub.com, you'll see a page with the app's developer contact information and a list of the specific data that's being requested.

Tip: You must verify your email address before you can authorize an OAuth app.

OAuth app access

OAuth apps can have *read* or *write* access to your GitHub Enterprise Cloud data.

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

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."

About OAuth scopes

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

When you want to use an OAuth app that integrates with GitHub Enterprise Cloud, that app lets you know what type of access to your data will be required. If you grant access to the app, then the app 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.

There is a limit of ten tokens that are issued per user/application/scope combination, and

a rate limit of ten tokens created per hour. If an application creates more than ten tokens for the same user and the same scopes, the oldest tokens with the same user/application/scope combination are revoked. However, hitting the hourly rate limit will not revoke your oldest token. Instead, it will trigger a re-authorization prompt within the browser, asking the user to double check the permissions they're granting your app. This prompt is intended to give a break to any potential infinite loop the app is stuck in, since there's little to no reason for an app to request ten tokens from the user within an hour.

Types of requested data

OAuth apps can request several types of data.

Type of data	Description
Commit status	You can grant access for an app to report your commit status. Commit status access allows apps to determine if a build is a successful against a specific commit. Apps won't have access to your code, but they can read and write status information against a specific commit.
Deployments	Deployment status access allows apps to determine if a deployment is successful against a specific commit for public and private repositories. Apps won't have access to your code.
Gists	Gist access allows apps to read or write to both your public and secret Gists.
Hooks	Webhooks access allows apps to read or write hook configurations on repositories you manage.
Notifications	Notification access allows apps to read your GitHub Enterprise Cloud notifications, such as comments on issues and pull requests. However, apps 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. Apps can request access for either public or private repositories on a user-wide level.
Repository delete	Apps can request to delete repositories that you administer, but they won't have access to your code.
Projects	Access to user and organization projects. Apps can request either read/write or read only access.

Requesting updated permissions

When OAuth apps request new access permissions, they will notify you of the differences between their current permissions and the new permissions.

OAuth apps and organizations

When you authorize an OAuth app for your personal account, you'll also see how the authorization will affect each organization you're a member of.

- **For organizations *with* OAuth app access restrictions, you can request that organization admins approve the application for use in that organization.** If the organization does not approve the application, then the application will only be able to access the organization's public resources. If you're an organization admin, you can approve the application yourself.
- **For organizations *without* OAuth app access restrictions, the application will automatically be authorized for access to that organization's resources.** For this reason, you should be careful about which OAuth apps you approve for access to your personal account resources as well as any organization resources.

If you belong to any organizations with SAML single sign-on (SSO) enabled, and you have created a linked identity for that organization by authenticating via SAML in the past, you must have an active SAML session for each organization each time you authorize an OAuth app.

> **Note:** If you're encountering issues with an authorized OAuth app or GitHub App accessing an organization that is protected by SAML, you may need to revoke the app from your Authorized GitHub Apps or Authorized OAuth apps page, visit the organization to authenticate and establish an active SAML session, and then attempt to reauthorize the app by accessing it.

Further reading

- "About OAuth app access restrictions"
- "Authorizing GitHub Apps"
- "GitHub Marketplace support"