Enabling OAuth app access restrictions for your organization

Organization owners can enable OAuth app access restrictions to prevent untrusted apps from accessing the organization's resources while allowing organization members to use OAuth apps for their personal accounts.

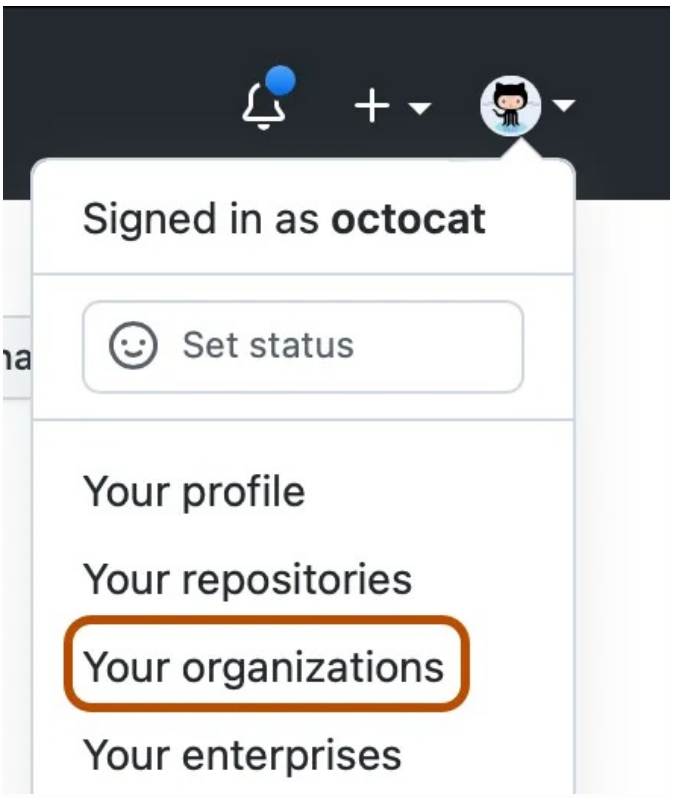
When you create a new organization, OAuth app access restrictions are enabled by default. Organization owners can disable OAuth app access restrictions at any time.

Even if you restrict OAuth apps access in your organization, users can still authorize internal OAuth apps and use them to access data from the organization. For more information, see "Internal OAuth apps."

Warnings:

- Enabling OAuth app access restrictions will revoke organization access for all previously authorized OAuth apps and SSH keys. For more information, see "About OAuth app access restrictions."
- Once you've set up OAuth app access restrictions, make sure to reauthorize any OAuth app that require access to the organization's private data on an ongoing basis. All organization members will need to create new SSH keys, and the organization will need to create new deploy keys as needed.
- When OAuth app access restrictions are enabled, applications can use an OAuth token to access information about GitHub Marketplace transactions.

1. In the top right corner of GitHub.com, click your profile photo, then click **Your organizations**.



2. Next to the organization, click **Settings**.
3. In the "Integrations" section of the sidebar, click **OAuth application policy**.
4. Under "Third-party application access policy," click **Setup application access restrictions**.
5. After you review the information about third-party access restrictions, click **Restrict third-party application access**.