About OAuth app access restrictions

In this article

Organizations can choose which OAuth apps have access to their repositories and other resources by enabling OAuth app access restrictions.

About OAuth app access restrictions

When OAuth app access restrictions are enabled, organization members and outside collaborators cannot authorize OAuth app access to organization resources. Organization members can request owner approval for OAuth apps they'd like to use, and organization owners receive a notification of pending requests.

Organization owners can choose whether to allow outside collaborators to request access for unapproved OAuth apps and GitHub Apps. For more information, see "Limiting OAuth app and GitHub App access requests."

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

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.

> **Tip**: When an organization has not set up OAuth app access restrictions, any OAuth app authorized by an organization member can also access the organization's private resources.

Setting up OAuth app access restrictions

When an organization owner sets up OAuth app access restrictions for the first time:

- **Applications that are owned by the organization** are automatically given access to the organization's resources.
- **OAuth apps** immediately lose access to the organization's resources.
- **SSH keys created before February 2014** immediately lose access to the organization's resources (this includes user and deploy keys).
- **SSH keys created by OAuth apps during or after February 2014** immediately lose access to the organization's resources.
- **Hook deliveries from private organization repositories** will no longer be sent

to unapproved OAuth apps.

- **API access** to private organization resources is not available for unapproved OAuth apps. In addition, there are no privileged create, update, or delete actions on public organization resources.
- **Hooks created by users and hooks created before May 2014** will not be affected.
- **Private forks of organization-owned repositories** are subject to the organization's access restrictions.

Resolving SSH access failures

When an SSH key created before February 2014 loses access to an organization with OAuth app access restrictions enabled, subsequent SSH access attempts will fail. Users will encounter an error message directing them to a URL where they can approve the key or upload a trusted key in its place.

Webhooks

When an OAuth app is granted access to the organization after restrictions are enabled, any pre-existing webhooks created by that OAuth app will resume dispatching.

When an organization removes access from a previously-approved OAuth app, any pre-existing webhooks created by that application will no longer be dispatched (these hooks will be disabled, but not deleted).

Re-enabling access restrictions

If an organization disables OAuth app access application restrictions, and later re-enables them, previously approved OAuth app are automatically granted access to the organization's resources.

Further reading

- "Enabling OAuth app access restrictions for your organization"
- "Approving OAuth apps for your organization"
- "Reviewing GitHub Apps installed in your organization"
- "Denying access to a previously approved OAuth app for your organization"
- "Disabling OAuth app access restrictions for your organization"
- "Requesting organization approval for OAuth apps"
- "Authorizing OAuth apps"