About programmatic access in your organization

In this article

As an organization owner, you can control access to your organization by personal access tokens, GitHub Apps, and OAuth apps.

Who can use this feature
Organization owners can control programmatic access in their organization.

About programmatic access 🔗

GitHub Apps, OAuth apps, and personal access tokens can be used to make API requests that read or write resources owned by an organization. As an organization owner, you can control access to your organization by GitHub Apps and personal access tokens.

GitHub Apps 🔗

Organization owners can install GitHub Apps on their organization. Repository admins can also install a GitHub App on the organization if the app does not request organization resources and if they only grant the app access to repositories where they are an admin. Organization members can submit a request for their organization owner to install a GitHub App on the organization. For more information, see "[Installing your own GitHub App](#)."

Organization owners can prevent outside collaborators from requesting GitHub Apps or from installing a GitHub App even if the collaborator is a repository admin. For more information, see "[Limiting OAuth app and GitHub App access requests](#)."

Organization owners can review the GitHub Apps that are installed on their organization and modify the repositories that each app can access. For more information, see "[Reviewing GitHub Apps installed in your organization](#)."

To help maintain GitHub Apps owned by their organization, organization owners can designate other users in their organization as GitHub App managers. GitHub App managers can manage the settings of some or all of the GitHub Apps that are owned by the organization. The GitHub App manager role does not grant users permission to install GitHub Apps on an organization. For more information, see "[Adding and removing GitHub App managers in your organization](#)."

Personal access tokens 🔗

Organization owners can prevent fine-grained personal access tokens and personal access tokens (classic) from accessing resources owned by the organization. Organization owners can also require approval for each fine-grained personal access token that can access the organization. For more information, see "[Setting a personal access token policy for your organization](#)."

Organization owners can view all fine-grained personal access tokens that can access resources owned by the organization. Organization owners can also revoke access by fine-grained personal access tokens. For more information, see "[Reviewing and revoking personal access tokens in your organization](#)."

Site administrators can use the REST API to manage personal access tokens in their enterprise. For more information, see "[Users](#)" in the REST API documentation.

Legal

© 2023 GitHub, Inc.   [Terms](#)   [Privacy](#)   [Status](#)   [Pricing](#)   [Expert services](#)   [Blog](#)