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, OAuth 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 a GitHub App from GitHub Marketplace for your organizations."

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."

OAuth apps

Organization managers can restrict OAuth apps from accessing organization resources. When these restrictions are enabled, organization members and outside collaborators can still request approval for individual OAuth apps. For more information, see "About OAuth app access restrictions."

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."

If their organization uses SAML, organization owners can see each personal access token that a member of their organization authorized. For more information, see "Viewing and managing a member's SAML access to your organization."