

Authenticating with a GitHub App

Learn how to authenticate with GitHub Apps.

About authentication with a GitHub App

Your GitHub App can authenticate as itself, as an app installation, or on behalf of a user.

Authenticating as a GitHub App

You can authenticate as a GitHub App in order to generate an installation access token or manage your app.

Authenticating as a GitHub App installation

You can make your GitHub App authenticate as an installation in order to make API requests that affect resources owned by the account where the app is installed.

Authenticating with a GitHub App on behalf of a user

Your GitHub App can perform actions on behalf of a user, like creating an issue, posting a comment, or creating a deployment.

Managing private keys for GitHub Apps

You can manage private keys to authenticate with your GitHub App.

Generating a JSON Web Token (JWT) for a GitHub App

Learn how to create a JSON Web Token (JWT) to authenticate to certain REST API endpoints with your GitHub App.

Generating an installation access token for a GitHub App

Learn how to generate an installation access token for your GitHub App.

Generating a user access token for a GitHub App

You can generate a user access token for your GitHub App in order to attribute app activity to a user.

Refreshing user access tokens

To enforce regular token rotation and reduce the impact of a compromised token, you can configure your GitHub App to use user access tokens that expire.

Making authenticated API requests with a GitHub App in a GitHub Actions workflow

You can use an installation access token from a GitHub App to make authenticated API requests in a GitHub Actions workflow. You can also pass the token to a custom action to enable the action to make authenticated API requests.

Legal

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