

About authentication with a GitHub App

In this article

- Authentication as a GitHub App
- Authentication as an app installation
- Authentication on behalf of a user

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

Authentication as a GitHub App [↗](#)

Your app should authenticate as itself when it needs to generate an installation access token. An installation access token is required to authenticate as an app installation. Your app should also authenticate as itself when it needs to make API requests to manage resources related to the app. For example, when it needs to list the accounts where it is installed. For more information, see "[Authenticating as a GitHub App](#)".

Authentication as an app installation [↗](#)

Your app should authenticate as an app installation when you want to attribute app activity to the app. Authenticating as an app installation lets your app access resources that are owned by the user or organization that installed the app. Authenticating as an app installation is ideal for automation workflows that don't involve user input. For more information, see "[Authenticating as a GitHub App installation](#)".

Authentication on behalf of a user [↗](#)

Your app should authenticate on behalf of a user when you want to attribute app activity to a user. Similar to authenticating as an app installation, your app can access resources that are owned by the user or organization that installed the app. Authenticating on behalf of a user is ideal when you want to ensure that your app only takes actions that could be performed by a specific user. For more information, see "[Authenticating with a GitHub App on behalf of a user](#)".

Legal