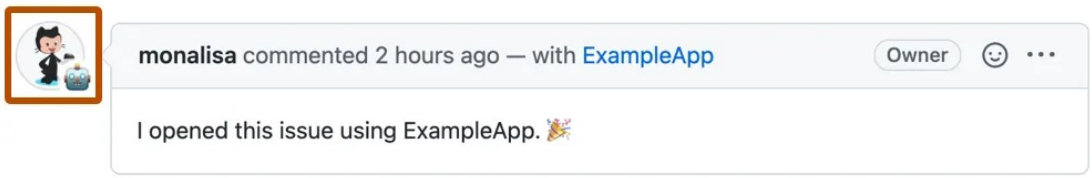
Authenticating with a GitHub App on behalf of a user

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

Your app can make API requests on behalf of a user. API requests made by an app on behalf of a user will be attributed to that user. For example, if your app posts a comment on behalf of a user, the GitHub UI will show the user's avatar photo along with the app's identicon badge as the author of the issue.



Similarly, if the request triggers a corresponding entry in the audit logs and security logs, the logs will list the user as the actor but will state that the "programmatic_access_type" is "GitHub App user-to-server token".

To make an API request on behalf of a user, the user must authorize your app. If an app is installed on an organization that includes multiple members, each member will need to authorize the app before the app can act on their behalf. An app does not need to be installed in order for a user to authorize the app.

When a user installs an app on their account or organization, they grant the app permission to access the organization and repository resources that it requested. During the installation process, they will also see a list of account permissions that the app can request for individual users. When a user authorizes an app, they grant the app permission to act on their behalf, and they grant the account permissions that the app requested.

Once a user has authorized your app, you can generate a user access token, which is a type of OAuth token. You should send the user access token in the `Authorization` header of your subsequent API requests. For more information about prompting a user to authorize your app and generating a user access token, see "Generating a user access token for a GitHub App."

Requests made with a user access token are sometimes called "user-to-server" requests.

If you want to attribute app activity to the app instead of to a user, you should authenticate as an app installation instead. For more information, see "Authenticating as a GitHub App installation."

Note: If a user reports that they cannot see resources owned by their organization after authorizing your GitHub App and the organization uses SAML SSO, instruct the user to start an active SAML session for their organization before reauthorizing. For more information, see "SAML and GitHub Apps."