

# Impersonating a user

## In this article

About user impersonation

Impersonating a user

---

You can impersonate users and perform actions on their behalf, for troubleshooting, unblocking, and other legitimate reasons.

### Who can use this feature

Enterprise owners can impersonate users within their enterprise.

## About user impersonation

If you need to temporarily take over a user account, for example when troubleshooting a user problem, or when the user is unavailable and urgent action is required, you can start an impersonation session to act on their behalf.

For each impersonation session, you need to provide a reason for the impersonation. A session is limited to one hour, and you will have the same access as the user being impersonated.

Actions you perform during an impersonation session are recorded as events in the enterprise audit log, as well as the impersonated user's security log. The person being impersonated is sent an email notification when the impersonation session starts. You cannot deactivate these emails. For more information, see "[Audit log events for your enterprise](#)" and "[Reviewing your security log](#)."

## Impersonating a user

- 1 From an administrative account on GitHub Enterprise Server, in the upper-right corner of any page, click .
- 2 If you're not already on the "Site admin" page, in the upper-left corner, click **Site admin**.
- 3 Under "Search users, organizations, teams, repositories, gists, and applications", type the name of the user in the text field.
- 4 To the right of text field, click **Search**.

Search users, organizations, teams, repositories, gists, and applications

Users are found by login, email, SSH key SHA256 fingerprint, GPG key, or database ID.

Organizations are found by login, email, or database ID.

Teams are found by organization/team, GraphQL object ID, or database ID.

Repositories are found by name, "username/repository", deploy key SHA256 fingerprint, or database ID.

Gists are found by name or "username/repository".

OAuth applications are found by name, client ID or application ID.

GitHub Apps are found by name or integration ID.

GitHub App installation are found by installation ID.

Webhooks are found by hook ID.

- If an exact account name match isn't found, under "Search results – Accounts", in the "Fuzzy matches" section, click the name of the user you want to manage.

Search results – Accounts

Fuzzy matches

 user2


 user1

- 5 Review the user details in the site admin page to confirm you have identified the correct user.

Site admin / user1

Admin
Security
Content
Collaboration

User info



user1 – View profile

user1@myexample.com and 0 more

Active

Security

Two-factor authentication disabled

No SSH keys and no GPG keys

No personal access tokens

Search audit logs

Repositories

No repositories

- 6 In the top left of the page, click **User info**.

👤 **User info**

👤 ghe-admin – [View profile](#)

✉ mona@github.com  
and 0 more

🕒 **Active**



🛡 **Security**

- ✕ Two-factor authentication disabled
- ✕ [No SSH keys](#) and [no GPG keys](#)
- ✕ [No personal access tokens](#)
- 🕒 [Search audit logs](#)

- 7 Under "Danger Zone", click **Sign in to GitHub as @username**
- 8 Select a reason from the dropdown list. If you select **Other** you will need to provide additional context in the text field below **Notes**. Click **Begin impersonation** to begin the session.
- 9 When you are ready to end the impersonation session, click **Return to your mundane life as username** in the banner at the top of the page.

## Legal

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