# Managing users in your enterprise

You can audit user activity and manage user settings.

## Roles in an enterprise

Everyone in an enterprise is a member of the enterprise. To control access to your enterprise's settings and data, you can assign different roles to members of your enterprise.

## Best practices for user security

Outside of instance-level security measures (SSL, subdomain isolation, configuring a firewall) that a site administrator can implement, there are steps your users can take to help protect your enterprise.

## Inviting people to manage your enterprise

You can add and remove enterprise owners for your enterprise account.

## Promoting or demoting a site administrator

Site administrators can promote any normal user account to a site administrator, as well as demote other site administrators to regular users.

## Viewing people in your enterprise

To audit access to enterprise-owned resources or user license usage, enterprise owners can view every administrator and member of the enterprise.

## Auditing users across your enterprise

The audit log dashboard shows site administrators the actions performed by all users and organizations across your enterprise within the current month and previous six months. The audit log includes details such as who performed the action, what the action was, and when the action was performed.

## Impersonating a user

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

## Managing dormant users

By default, a user account is considered to be dormant if it has not been active for 90 days. You can configure the length of time a user must be inactive to be considered dormant and choose to suspend dormant users to release user licenses.

### Suspending and unsuspending users

If a user leaves or moves to a different part of the company, you should remove or modify their ability to access your GitHub Enterprise Server instance.

### Placing a legal hold on a user or organization

You can place a legal hold on a user or organization to ensure that repositories they own cannot be permanently removed from your enterprise.

### Auditing SSH keys

Site administrators can initiate an instance-wide audit of SSH keys.

### Rebuilding contributions data

You may need to rebuild contributions data to link existing commits to a user account.