

Managing security settings for your organization

You can manage security settings and review the audit log, compliance reports, and integrations for your organization.

Managing security and analysis settings for your organization

You can control features that secure and analyze the code in your organization's projects on GitHub.

Managing allowed IP addresses for your organization

You can restrict access to your organization's private assets by configuring a list of IP addresses that are allowed to connect.

Restricting email notifications for your organization

To prevent organization information from leaking into personal email accounts, you can restrict the domains where members can receive email notifications about organization activity.

Reviewing the audit log for your organization

The audit log allows organization admins to quickly review the actions performed by members of your organization. It includes details such as who performed the action, what the action was, and when it was performed.

Identifying audit log events performed by an access token

You can identify the actions performed by a specific token in your organization.

Displaying IP addresses in the audit log for your organization

You can display the source IP address for events in your organization's audit log.

Audit log events for your organization

Learn about audit log events recorded for your organization.

Accessing compliance reports for your organization

You can access GitHub's compliance reports, such as our SOC reports and Cloud Security Alliance CAIQ self-assessment (CSA CAIQ), for your organization.

Legal