Displaying IP addresses in the audit log for your enterprise

In this article

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

> **Who can use this feature**
> Enterprise owners can display IP addresses in the audit log for an enterprise.

About display of IP addresses in the audit log

By default, GitHub Enterprise Cloud does not display the source IP address for events in your enterprise's audit log. Optionally, to ensure compliance and respond to threats, you can display the full IP address associated with the actor responsible for each event. Actors are typically users, but can also be apps or integrations.

You are responsible for meeting any legal obligations that accompany the viewing or storage of IP addresses displayed within your enterprise's audit log.

If you choose to display IP addresses for your enterprise account, the IP addresses will appear in both your enterprise's audit log and the audit log of every organization owned by your enterprise. Alternatively, you can enable the display of IP addresses in the audit log for individual organizations. For more information, see "Displaying IP addresses in the audit log for your organization."

You can display IP addresses in the audit log regardless of which authentication method you use for your enterprise on GitHub.com. For more information, see "About authentication for your enterprise."

When anyone creates an account on GitHub.com, the person agrees to GitHub's collection of basic information about connections to GitHub's services, including source IP address. For more information, see "GitHub Privacy Statement."

Events that display IP addresses in the audit log

GitHub Enterprise Cloud displays an IP address in the audit log when a member of the enterprise interacts with a resource owned by your enterprise or an organization in your enterprise. For example, you will see an IP address for audited events involving an internal or private repository owned by an organization in your enterprise, or resources associated with those repositories, such as an issue, pull request, action, or project.

If members of your enterprise access GitHub.com with personal accounts that they manage, because you do not use Enterprise Managed Users, GitHub Enterprise Cloud does not display an event or IP address in the audit log for the following actions.

- Authentication to GitHub.com
- Interactions with a resource owned by the personal account, including a repository, gist, or project
- Interactions with a public repository owned by an organization in your enterprise

Enabling display of IP addresses in the audit log

1. In the top-right corner of GitHub.com, click your profile photo, then click **Your enterprises**.
2. In the list of enterprises, click the enterprise you want to view.
3. In the enterprise account sidebar, click ⚙ **Settings**.
4. Under "⚙ Settings", click **Audit log**.
5. Under "Audit log", click **Settings**.
6. Under "Disclose actor IP addresses in audit logs", select **Enable source IP disclosure**.
7. Click **Save**.

After you enable the feature, you can access the audit log to view events that include IP addresses. For more information, see "Accessing the audit log for your enterprise."