Best practices for user security

In this article

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.

Enabling two-factor authentication

Two-factor authentication (2FA) is a way of logging in to websites and services that requires a second factor beyond a password for authentication. In GitHub Enterprise Server's case, this second factor is a one time authentication code generated by an application on a user's smartphone. We strongly recommend requiring your users to enable two-factor authentication on their accounts. With two-factor authentication, both a user's password and their smartphone would have to be compromised to allow the account itself to be compromised.

For more information on configuring two-factor authentication, see "About two-factor authentication".

Requiring a password manager

We strongly recommend requiring your users to install and use a password manager on any computer they use to connect to your enterprise. Doing so ensures that passwords are stronger and much less likely to be compromised or stolen.

Restrict access to teams and repositories

To limit the potential attack surface in the event of a security breach, we strongly recommend only giving users access to teams and repositories that they absolutely need to do their work. Since members with the Owner role can access all teams and repositories in the organization, we strongly recommend keeping this team as small as possible.

For more information on configuring teams and team permissions, see "Roles in an organization."