This version of GitHub Enterprise was discontinued on 2023-03-15. No patch releases will be made, even for critical security issues. For better performance, improved security, and new features, upgrade to the latest version of GitHub Enterprise. For help with the upgrade, contact GitHub Enterprise support.

About pre-receive hooks

In this article

Pre-receive hooks are scripts that run on the GitHub Enterprise Server appliance that you can use to implement quality checks.

About pre-receive hooks

When a push occurs, each script runs in an isolated environment and can perform checks on the content of the push. The scripts will cause the push to be accepted if the exit status is 0, or rejected if the exit status is non-zero.

Use pre-receive hooks to satisfy business rules, enforce regulatory compliance, and prevent certain common mistakes.

Examples of how you can use pre-receive hooks:

- Require commit messages to follow a specific pattern or format, such as including a valid ticket number or being over a certain length.
- Lock a branch or repository by rejecting all pushes.
- Prevent sensitive data from being added to the repository by blocking keywords, patterns or file types.
- Prevent a PR author from merging their own changes.

You can see examples of pre-receive hooks for GitHub Enterprise Server in the `github/platform-samples` repository.

Impact on performance and workflows

Impact to developers and their workflows can be significant and must be considered carefully. Pre-receive hooks that are based on business needs and implemented thoughtfully will provide the most benefit to the organization as a whole.

Pre-receive hooks can have unintended effects on the performance of your GitHub Enterprise Server instance and should be carefully implemented and reviewed.