Enterprise administrators / Code security / GitHub Advanced Security / Configuring dependency review

Configuring dependency review for your appliance

Configure GitHub Advanced Security
4 of 6 in learning path

Next: **Configuring secret scanning for your appliance**

In this article

To help users understand dependency changes when reviewing pull requests, you can enable, configure, and disable dependency review for your GitHub Enterprise Server instance.

Dependency review is available for organization-owned repositories in GitHub Enterprise Server. This feature requires a license for GitHub Advanced Security. For more information, see "About GitHub Advanced Security."

About dependency review

Dependency review helps you understand dependency changes and the security impact of these changes at every pull request. It provides an easily understandable visualization of dependency changes with a rich diff on the "Files Changed" tab of a pull request. Dependency review informs you of:

- Which dependencies were added, removed, or updated, along with the release dates.
- How many projects use these components.
- Vulnerability data for these dependencies.

Some additional features, such as license checks, blocking of pull requests, and CI/CD integration, are available with the dependency review action.

Checking whether your license includes GitHub Advanced Security

You can identify if your enterprise has a GitHub Advanced Security license by reviewing your enterprise settings. For more information, see "Enabling GitHub Advanced Security for your enterprise."

Prerequisites for dependency review

- A license for GitHub Advanced Security (see "About billing for GitHub Advanced Security").
- The dependency graph enabled for the instance. Site administrators can enable the dependency graph via the management console or the administrative shell (see "Enabling the dependency graph for your enterprise").
- GitHub Connect enabled to download and synchronize vulnerabilities from the GitHub Advisory Database. This is usually configured as part of setting up Dependabot (see "Enabling Dependabot for your enterprise").

Enabling and disabling dependency review

To enable or disable dependency review, you need to enable or disable the dependency graph for your instance.

For more information, see "Enabling the dependency graph for your enterprise."

Running dependency review using GitHub Actions

Note: The dependency review action is currently in public beta and subject to change.

The dependency review action is included in your installation of GitHub Enterprise Server. It is available for all repositories that have GitHub Advanced Security and dependency graph enabled.

The dependency review action scans your pull requests for dependency changes and raises an error if any new dependencies have known vulnerabilities. The action is supported by an API endpoint that compares the dependencies between two revisions and reports any differences.

For more information about the action and the API endpoint, see the `dependency-review-action` documentation, and "Dependency review" in the API documentation.

Users run the dependency review action using a GitHub Actions workflow. If you have not already set up runners for GitHub Actions, you must do this to enable users to run workflows. You can provision self-hosted runners at the repository, organization, or enterprise account level. For information, see "About self-hosted runners" and "Adding self-hosted runners."

Previous
Configuring code scanning for your appliance

Next
Configuring secret scanning for your appliance