

# Enabling Dependabot for your enterprise

## In this article

About Dependabot for GitHub Enterprise Server

Enabling Dependabot alerts

Enabling Dependabot updates

You can allow users of your GitHub Enterprise Server instance to find and fix vulnerabilities in code dependencies by setting up Dependabot alerts and Dependabot updates.

## Who can use this feature

Enterprise owners can set up Dependabot.

## About Dependabot for GitHub Enterprise Server [↗](#)

Dependabot helps users of your GitHub Enterprise Server instance find and fix vulnerabilities in their dependencies. You must first set up Dependabot for your enterprise, and then you can enable Dependabot alerts to notify users about vulnerable dependencies and Dependabot updates to fix the vulnerabilities and keep dependencies updated to the latest version.

Dependabot is just one of many features available to harden supply chain security for your GitHub Enterprise Server instance. For more information about the other features, see "[About supply chain security for your enterprise](#)."

## About Dependabot alerts [↗](#)

With Dependabot alerts, GitHub identifies insecure dependencies in repositories and creates alerts on your GitHub Enterprise Server instance, using data from the GitHub Advisory Database and the dependency graph service.

We add advisories to the GitHub Advisory Database from the following sources:

- Security advisories reported on GitHub
- The [National Vulnerability database](#)
- The [npm Security advisories database](#)
- The [FriendsOfPHP database](#)
- The [Go Vulncheck database](#)
- The [Python Packaging Advisory database](#)
- The [Ruby Advisory database](#)
- The [RustSec Advisory database](#)
- Community contributions. For more information, see <https://github.com/github/advisory-database/pulls>.

If you know of another database we should be importing advisories from, tell us about it by opening an issue in <https://github.com/github/advisory-database>.

After you set up Dependabot for your enterprise, vulnerability data is synced from the GitHub Advisory Database to your instance once every hour. Only GitHub-reviewed advisories are synchronized. For more information, see "[Browsing security advisories in the GitHub Advisory Database](#)."

You can also choose to manually sync vulnerability data at any time. For more information, see "[Viewing the vulnerability data for your enterprise](#)."

**Note:** When you enable Dependabot alerts, no code or information about code from your GitHub Enterprise Server instance is uploaded to GitHub.com.

When your GitHub Enterprise Server instance receives information about a vulnerability, it identifies repositories in your GitHub Enterprise Server instance that use the affected version of the dependency and generates Dependabot alerts. You can choose whether or not to notify users automatically about new Dependabot alerts.

For repositories with Dependabot alerts enabled, scanning is triggered on any push to the default branch that contains a manifest file or lock file. Additionally, when a new vulnerability record is added to your GitHub Enterprise Server instance, GitHub Enterprise Server scans all existing repositories on your GitHub Enterprise Server instance and generates alerts for any repository that is vulnerable. For more information, see "[About Dependabot alerts](#)."

## About Dependabot updates

After you enable Dependabot alerts, you can choose to enable Dependabot updates. When Dependabot updates are enabled for your GitHub Enterprise Server instance, users can configure repositories so that their dependencies are updated and kept secure automatically.

**Note:** Dependabot updates on GitHub Enterprise Server requires GitHub Actions with self-hosted runners.

By default, GitHub Actions runners used by Dependabot need access to the internet, to download updated packages from upstream package managers. For Dependabot updates powered by GitHub Connect, internet access provides your runners with a token that allows access to dependencies and advisories hosted on GitHub.com.

You can enable Dependabot updates for specific private registries on GitHub Enterprise Server instances with limited, or no, internet access. For more information, see "[Configuring Dependabot to work with limited internet access](#)."

With Dependabot updates, GitHub automatically creates pull requests to update dependencies in two ways.

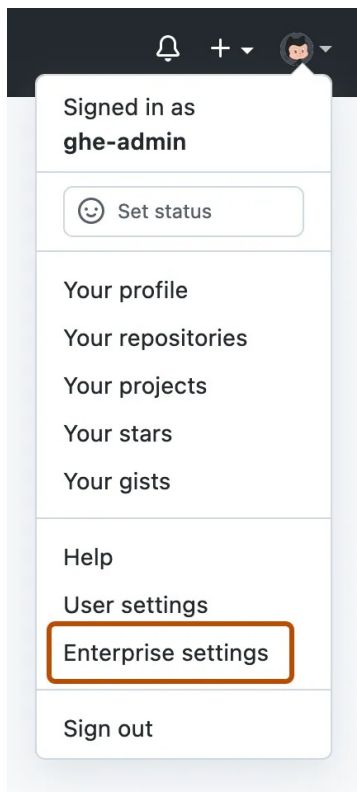
- **Dependabot version updates:** Users add a Dependabot configuration file to the repository to enable Dependabot to create pull requests when a new version of a tracked dependency is released. For more information, see "[About Dependabot version updates](#)."
- **Dependabot security updates:** Users toggle a repository setting to enable Dependabot to create pull requests when GitHub detects a vulnerability in one of the dependencies of the dependency graph for the repository. For more information, see "[About Dependabot alerts](#)" and "[About Dependabot security updates](#)."

## Enabling Dependabot alerts

Before you can enable Dependabot alerts, you must first set up Dependabot for your enterprise:

- You must enable GitHub Connect. For more information, see "[Managing GitHub Connect](#)."
- You must enable the dependency graph. For more information, see "[Enabling the dependency graph for your enterprise](#)."

- 1 In the top-right corner of GitHub Enterprise Server, click your profile photo, then click **Enterprise settings**.



- 2 In the enterprise account sidebar, click  **GitHub Connect**.

- 3 Under "Dependabot", to the right of "Periodically download the GitHub Advisory Database so that users can receive vulnerability alerts for open source code dependencies", select the dropdown menu and click **Enabled without notifications**. Optionally, to enable alerts with notifications, click **Enabled with notifications**.

#### Dependabot

Periodically download the GitHub Advisory Database so that users can receive vulnerability alerts for open source code dependencies.

After enabling, repository and organization admins can enable Dependabot alerts for each repository or organization. [Learn more](#).

Disable ▾

#### Unified contributions

Users can send contribution counts for their activity to their selected GitHub.com profile. [Learn more](#).

✓ Enable with notifications

Enable without notifications

Disable

**Tip:** We recommend configuring Dependabot alerts without notifications for the first few days to avoid an overload of emails. After a few days, you can enable notifications to receive Dependabot alerts as usual.

You can now enable Dependabot alerts for all existing or new private and internal repositories in the enterprise settings page for "Code security and analysis."

Alternatively, repository administrators and organization owners can enable Dependabot alerts for each repository and organization. Public repositories are always enabled by default. For more information, see "[Configuring Dependabot alerts](#)."



## Enabling Dependabot updates

After you enable Dependabot alerts for your enterprise, you can enable Dependabot updates.

Before you enable Dependabot updates, you must configure your GitHub Enterprise Server instance to use GitHub Actions with self-hosted runners. For more information, see "[Getting started with GitHub Actions for GitHub Enterprise Server](#)."

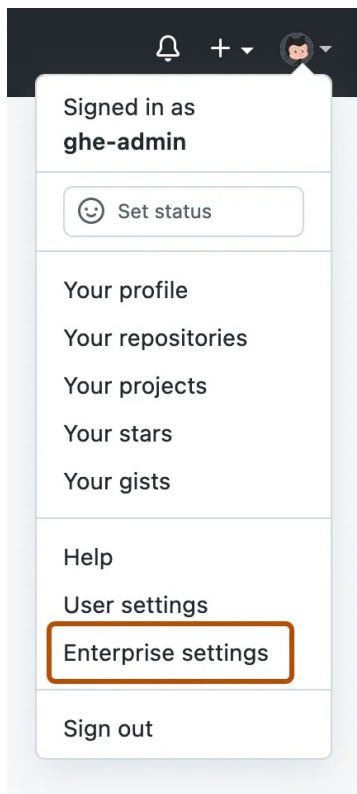
Dependabot updates are not supported on GitHub Enterprise Server if your enterprise uses clustering.


**Note:** After you enable the dependency graph, you can use the [Dependabot action](#). The action will raise an error if any vulnerabilities or invalid licenses are being introduced. For more information about the action, and for instructions about how to download the most recent version, see "[Using the latest version of the official bundled actions](#)."

- 1 Sign in to your GitHub Enterprise Server instance at `http(s)://HOSTNAME/login`.
- 2 From an administrative account on GitHub Enterprise Server, in the upper-right corner of any page, click .
- 3 If you're not already on the "Site admin" page, in the upper-left corner, click **Site admin**.
- 4 In the " Site admin" sidebar, click **Management Console**.
- 5 In the "Settings" sidebar, click **Security**.
- 6 Under "Security", select **Dependabot security updates**.
- 7 Under the "Settings" sidebar, click **Save settings**.

**Note:** Saving settings in the Management Console restarts system services, which could result in user-visible downtime.

- 8 Wait for the configuration run to complete.
- 9 Click **Visit your instance**.
- 10 Configure dedicated self-hosted runners to create the pull requests that will update dependencies. This is required because the workflows use a specific runner label. For more information, see "[Managing self-hosted runners for Dependabot updates on your enterprise](#)."
- 11 In the top-right corner of GitHub Enterprise Server, click your profile photo, then click **Enterprise settings**.



- 12 In the enterprise account sidebar, click  **GitHub Connect**.
- 13 Under "Dependabot", to the right of "Users can easily upgrade to non-vulnerable open source code dependencies", click **Enable**.

When you enable Dependabot alerts, you should consider also setting up GitHub Actions for Dependabot security updates. This feature allows developers to fix vulnerabilities in their dependencies. For more information, see "[Managing self-hosted runners for Dependabot updates on your enterprise](#)."

If you need enhanced security, we recommend configuring Dependabot to use private registries. For more information, see "[Configuring access to private registries for Dependabot](#)."

## Legal

© 2023 GitHub, Inc. [Terms](#) [Privacy](#) [Status](#) [Pricing](#) [Expert services](#) [Blog](#)