Configuring Dependabot security updates

In this article

You can use Dependabot security updates or manual pull requests to easily update vulnerable dependencies.

Note: Your site administrator must set up Dependabot updates for your GitHub Enterprise Server instance before you can use this feature. For more information, see "Enabling Dependabot for your enterprise."

You may not be able to enable or disable Dependabot updates if an enterprise owner has set a policy at the enterprise level. For more information, see "Enforcing policies for code security and analysis for your enterprise."

About configuring Dependabot security updates

You can enable Dependabot security updates for any repository that uses Dependabot alerts and the dependency graph. For more information, see "About Dependabot security updates."

You can enable or disable Dependabot security updates for an individual repository, for a selection of repositories in an organization, or for all repositories owned by your personal account or organization. For more information about enabling security features in an organization, see "Securing your organization."

Supported repositories

GitHub automatically enables Dependabot security updates for newly created repositories if your personal account or organization has enabled **Automatically enable for new repositories** for Dependabot security updates. For more information, see "Managing Dependabot security updates for your repositories."

If you create a fork of a repository that has security updates enabled, GitHub will automatically disable Dependabot security updates for the fork. You can then decide whether to enable Dependabot security updates on the specific fork.

If security updates are not enabled for your repository and you don't know why, first try enabling them using the instructions given in the procedural sections below. If security updates are still not working, you can contact your site administrator.

Managing Dependabot security updates for your repositories

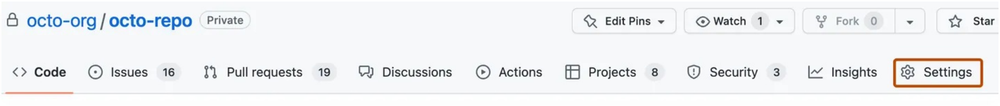
You can enable or disable Dependabot security updates for all qualifying repositories owned by your personal account or organization. For more information, see "Managing security and analysis settings for your personal account" or "Managing security and analysis settings for your organization."

You can also enable or disable Dependabot security updates for an individual repository.

Enabling or disabling Dependabot security updates for an individual repository

1. On your GitHub Enterprise Server instance, navigate to the main page of the repository.

2. Under your repository name, click ⚙ **Settings**. If you cannot see the "Settings" tab, select the ··· dropdown menu, then click **Settings**.



3. In the "Security" section of the sidebar, click **Code security and analysis**.

4. Under "Code security and analysis", to the right of "Dependabot security updates", click **Enable** to enable the feature or **Disable** to disable it.

Overriding the default behavior with a configuration file

You can override the default behavior of Dependabot security updates by adding a `dependabot.yml` file to your repository. For more information, see "Configuration options for the dependabot.yml file."

If you only require security updates and want to exclude version updates, you can set `open-pull-requests-limit` to `0` in order to prevent version updates for a given `package-ecosystem`. For more information, see "Configuration options for the dependabot.yml file."

```
# Example configuration file that:
#  - Has a private registry
#  - Ignores lodash dependency
#  - Disables version-updates

version: 2
registries:
  example:
    type: npm-registry
    url: https://example.com
    token: ${{secrets.NPM_TOKEN}}
updates:
  - package-ecosystem: "npm"
    directory: "/src/npm-project"
    schedule:
      interval: "daily"
    ignore:
      - dependency-name: "lodash"
```

```
        # For Lodash, ignore all updates
    # Disable version updates for npm dependencies
    open-pull-requests-limit: 0
    registries:
      - example
```

Note: In order for Dependabot to use this configuration for security updates, the `directory` must be the path to the manifest files, and you should not specify a `target-branch`.

For more information about the configuration options available for security updates, see the table in "Configuration options for the dependabot.yml file."

Further reading

- "About Dependabot alerts"
- "Configuring Dependabot alerts"
- "About the dependency graph"