Configuring tag protection rules

In this article

You can configure tag protection rules for your repository to prevent contributors from creating or deleting tags.

Tag protection rules are available in public repositories with GitHub Free and GitHub Free for organizations, and in public and private repositories with GitHub Pro, GitHub Team, GitHub Enterprise Cloud, and GitHub Enterprise Server. For more information, see "GitHub's plans."

Note: Tag protection rules are currently in beta and subject to change.

About tag protection rules

When you add a tag protection rule, all tags that match the pattern provided will be protected. Only users with admin or maintain permissions, or custom roles with the "edit repository rules" permission in the repository will be able to create protected tags, and only users with admin permissions or custom roles with the "edit repository rules" permission in the repository will be able to delete protected tags. For more information, see "Repository roles for an organization." GitHub Apps require the `Repository administration: write` permission to modify a protected tag.

Additionally, you can create custom repository roles to allow other groups of users to create or delete tags that match tag protection rules. For more information, see "Managing custom repository roles for an organization."

About importing tag protection rules to repository rulesets

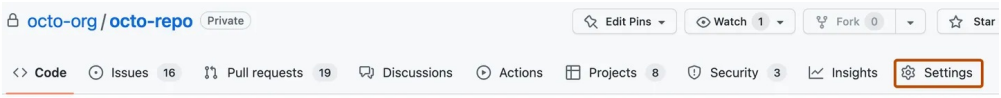
You can import existing tag protection rules into repository rulesets. This will implement the same tag protections you currently have in place for your repository. For more information, see "Importing tag protection rules to repository rulesets."

Rulesets have the following advantages over tag protection rules.

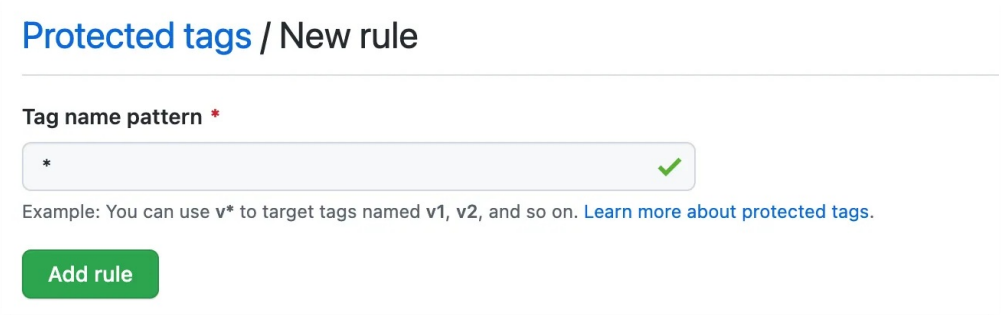
- Unlike protection rules, multiple rulesets can apply at the same time, so you can be confident that every rule targeting a tag in your repository will be evaluated when someone interacts with that tag. For more information, see "About rulesets."
- Rulesets have statuses, so you can easily manage which rulesets are active in a repository without needing to delete rulesets.
- Anyone with read access to a repository can view the active rulesets for the repository. This means a developer can understand why they have hit a rule, or an auditor can check the security constraints for the repository, without requiring admin access to the repository.
- With rulesets, you can restrict tag names on an organization-wide basis.

Adding tag protection rules

1. On GitHub.com, 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**.



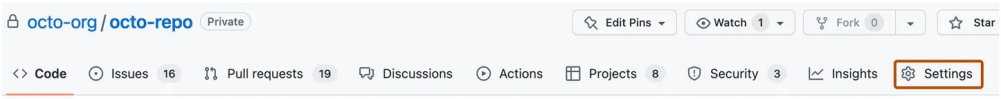
3. In the "Code and automation" section of the sidebar, click **Tags**.
4. Click **New rule**.
5. Under "Tag name pattern", type the pattern of the tags you want to protect. Tag protection rules use `fnmatch` syntax. For information about syntax options, see the fnmatch documentation. In this example, typing "*" protects all tags.



6. Click **Add rule**.

Importing tag protection rules to repository rulesets

1. On GitHub.com, 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 "Code and automation" section of the sidebar, click **Tags**.
4. Click **Import to rulesets** in the upper right corner.
5. Select **Create separate rulesets for creating and deleting protected tags** or **Create one ruleset for all protected tag operations**. Once created, the rulesets can be edited to further refine their behavior.
6. Click **Import**.