Securing your organization

In this article

You can use a number of GitHub features to help keep your organization secure.

> **Who can use this feature**
> Organization owners and security managers can manage security features for an organization.

Introduction 🔗

As an organization owner or security manager, you can use GitHub's security features to keep your organization's code, dependencies, and secrets secure. For more information, see "GitHub security features."

Your organization's security needs are unique. You may want to enable a feature if your organization has been impacted by a vulnerability that a certain feature would have prevented, or if the feature will help your organization meet a compliance requirement.

You can enable security features across multiple repositories in an organization at the same time. For each feature you want to enable, you must decide how to roll out the feature across your organization's repositories. Different features have different effects on your organization and its contributors, so it's important to assess the impact each feature will have. For example:

- Some features can generate notifications to inform your organization's members about specific vulnerabilities: to ensure these notifications are targeted and relevant, you may want to ask members to check their notification settings before you enable a feature. For more information, see "Configuring notifications."
- Some features can consume resources for each repository in which they're enabled. For example, enabling code scanning in a private repository may consume a GitHub Advanced Security license, and running code scanning analysis in a repository will incur usage of GitHub Actions or another CI system.

As an organization owner, you can give certain users permission to enable or disable security features by assigning the "security manager" role to a team. Security managers can configure security settings and monitor usage of security features across your organization. For more information, see "Managing security managers in your organization."

About prerequisites of features 🔗

Some security features have prerequisites. For example, Dependabot alerts use

information from the dependency graph, so enabling Dependabot alerts automatically enables the dependency graph.

Some features are only available to enterprises that use GitHub Advanced Security and have enabled Advanced Security as a feature for repositories. For more information, see "About GitHub Advanced Security."

> **Note:** Enterprises can set a policy to manage which organizations can enable GitHub Advanced Security. For more information, see "Enforcing policies for code security and analysis for your enterprise."

There are some features you must configure for each repository individually. For example, to enable Dependabot version updates in a repository, you must add a `dependabot.yml` file specifying where to find information about the project's dependencies. For more information, see "Configuring Dependabot version updates."

Enabling security features in your organization 🔗

When you have decided to enable a security feature, the next step is to decide how to roll out that feature across your organization.

- If you want to roll out a feature as quickly as possible, you can enable it for all eligible repositories at once. For more information, see "Enabling a feature for all repositories."
- If you want control over how quickly you roll out a feature, and which features are enabled in which repositories, you can enable a feature for a selection of repositories. For more information, see "Enabling a feature for a selection of repositories."

When you have decided how to enable a feature for your organization's existing repositories, you must also decide how to handle any new repositories that are created in your organization in the future. For more information, see "Enabling a feature for new repositories."

For more information about creating a strategy for rolling out security features across a large organization or enterprise, see "Introduction to adopting GitHub Advanced Security at scale."
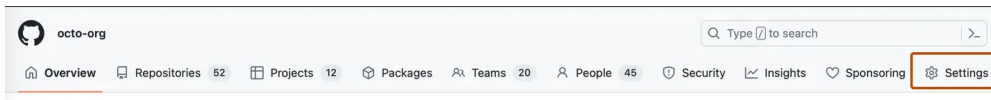
Enabling a feature for all repositories 🔗

The quickest way to roll out a security feature is to enable it for all repositories in your organization at once. If you've identified a critical need for a feature, enabling it for all repositories offers you protection across your entire organization, without requiring you to pause to devise a rollout plan.

Before you enable a feature for all repositories, you should consider the impact this action will have. If you're not sure about the effects a feature will have, it is safest to start by enabling the feature for a limited selection of repositories. Enabling a feature for all repositories at once is likely to be a suitable option in the following situations.

- You have an overview of all the repositories in your organization, and you're confident that they'll all benefit from a certain feature.
- If a feature requires resources such as GitHub Advanced Security licenses or GitHub Actions minutes, you have assessed the resources that will be required and are happy to proceed.
- If the feature generates notifications or pull requests, you're confident that these will be targeted and relevant for the members who receive them or have to review them.

When you're ready to proceed, follow these steps to enable a feature for all repositories.

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

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

3. In the left sidebar, click ⊕ **Code security and analysis**.

4. To enable a feature in all repositories in your organization where the feature is supported, next to the name of the feature, click **Enable all**.

When you click **Enable all**, you'll be prompted to confirm your choice. You'll also be told if the feature depends on another feature, or requires GitHub Advanced Security. For more information, see "Managing security and analysis settings for your organization."

Enabling a feature for a selection of repositories 🔗

In some cases, it is better to identify a selection of repositories that require a feature, then enable the feature just for those repositories.

If you're not sure about the impact a feature will have, you may want to test the feature on a limited selection of repositories before you commit to enabling the feature for all repositories, or you may want to roll out the feature gradually over several phases. You may also be aware that some repositories in your organization require a different set of features than others.

You can use the "Security coverage" view to identify repositories that require a certain feature, then enable the feature for those repositories. The following steps describe how to find the "Security coverage" view.

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

2. Under your organization name, click ⓘ **Security**.
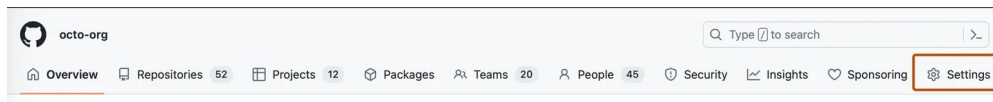

3. In the sidebar, click ⊘ **Coverage**.

On this view, you can use checkboxes to select specific repositories, or you can use the search bar to find the repositories where you want to enable a feature. For example, you can use filters to identify repositories where a certain team has write or admin access, or exclude repositories that don't require the same level of protection, such as test repositories or repositories for internal documentation. Then you can enable features for all selected repositories at once. For more information, see "Enabling security features for multiple repositories."

If you have a limited number of licenses for GitHub Advanced Security, you may want to prioritize repositories that contain critical projects, or that have the highest commit frequencies. For more information, see "About billing for GitHub Advanced Security."

Enabling a feature for new repositories 🔗

You can choose to enable a security feature automatically in all new repositories that are created in your organization. Enabling features in new repositories ensures they are protected immediately, and ensures any vulnerabilities in the repositories are identified as early as possible. However, to use security features as efficiently as possible, you may prefer to review each new repository individually.

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

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

3. In the left sidebar, click ⊙ **Code security and analysis**.

4. Below the name of the feature, select the option for automatically enabling the feature in applicable future repositories.

Monitoring the impact of security features 🔗

When you have enabled a feature, you should communicate with repository administrators and contributors in your organization to assess the impact of the feature. You may need to adjust the configuration of some features at the repository level, or reassess the distribution of security features across your organization. You should also monitor the security alerts that a feature generates, and your members' responses to these alerts.

You can use security overview to see which teams and repositories are affected by security alerts, with a breakdown of alerts by severity. For more information, see "Assessing your code security risk."

You can use various tools to monitor the actions that your organization's members are taking in response to security alerts. For more information, see "Auditing security alerts".

Next steps 🔗

To help users report security vulnerabilities, you can create a default security policy that will display in any of your organization's public repositories that do not have their own security policy. For more information, see "Creating a default community health file."

Once your organization's security setup is in place, you may want to prevent users from changing the security settings in a repository. An enterprise owner can prevent

repository administrators from enabling or disabling features in a repository. For more information, see "[Enforcing policies for code security and analysis for your enterprise](#)."

Legal

[Terms](#)   [Privacy](#)   [Status](#)   [Pricing](#)   [Expert services](#)   [Blog](#)