

Enabling security features for multiple repositories

In this article

About enabling security features

Enabling security features for multiple repositories

You can use security overview to select a subset of repositories and enable security features for them all.

Who can use this feature

Security overview for an organization is available to all members of the organization. The views and data displayed are determined by your role in the organization, and by your permissions for individual repositories within the organization. For more information, see "[About security overview](#)."

Security overview for an enterprise shows organization owners and security managers data for the organizations they have access to. Enterprise owners can only view data for organizations where they are added as an organization owner or security manager. For more information, see "[Managing your role in an organization owned by your enterprise](#)."

All enterprises and their organizations have a security overview. If you use GitHub Advanced Security features, which are free for public repositories, you will see additional information. For more information, see "[About GitHub Advanced Security](#)."

About enabling security features

If you're a security manager, repository administrator, or organization owner, you can use security overview to enable or disable security features for multiple repositories at the same time. You can enable or disable security features for all repositories visible on the "Security coverage" view in security overview for an organization.


You can use checkboxes to select which repositories you want to include, or use the search bar to narrow down to a specific subset of repositories, and enable or disable security features for that group. This is useful if you want to introduce a feature to your organization gradually over time, or if your organization requires a complex security setup where different features are enabled in different repositories. For example, if you are enabling a feature across a group of repositories, you may find the following filtering options helpful.

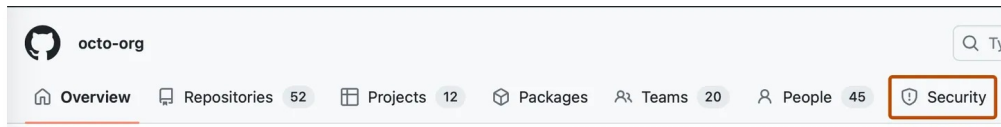
- To exclude certain repositories from the selection, you can assign a topic such as `test` to these repositories, then exclude them from the results with a search like `-topic:test`. For more information, see "[Classifying your repository with topics](#)."
- If a team uses repositories that all require a certain feature, you can use the `team:` filter to search for repositories where a team has write or admin access.
- If you're enabling code scanning, you can see which repositories are eligible for default setup with the search `code-scanning-default-setup:eligible`. For more information, see "[Configuring default setup for code scanning at scale](#)."


For more information on filters you can use in different parts of security overview, see "[Filtering alerts in security overview](#)."

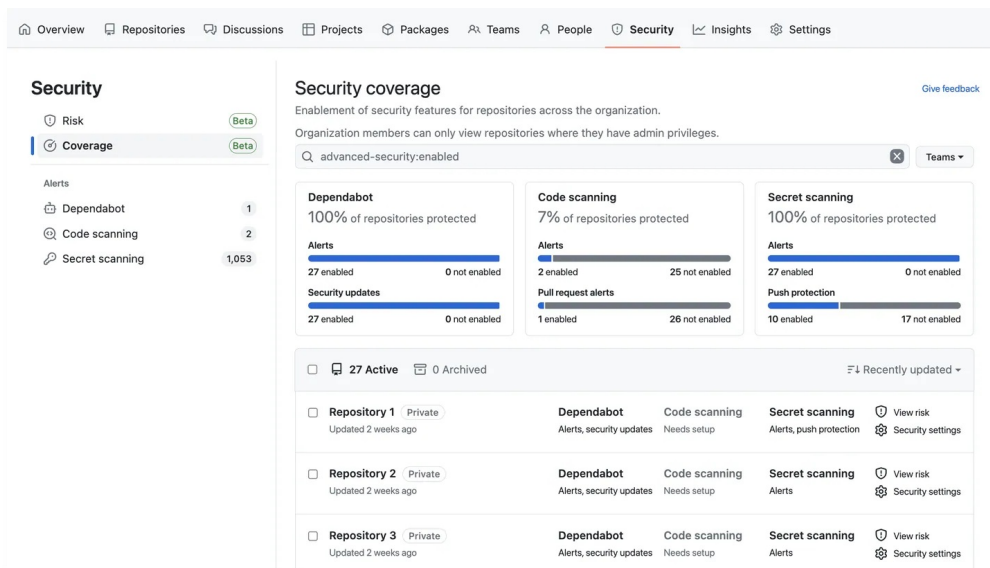
For more information about the different ways of enabling security features in an organization, see "[Securing your organization](#)."

Enabling security features for multiple repositories

- 1 On GitHub.com, navigate to the main page of the organization.
- 2 Under your organization name, click  **Security**.

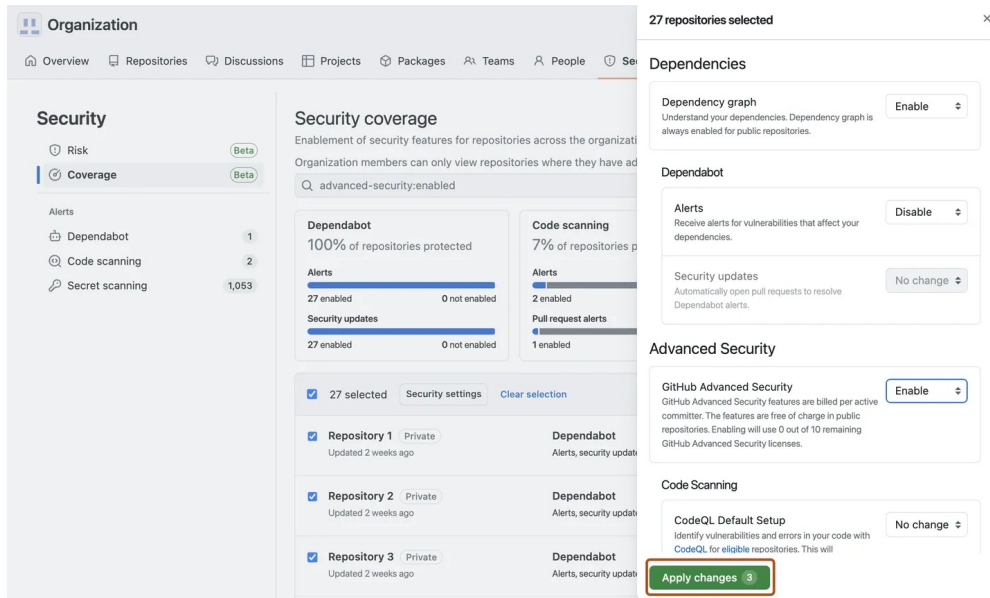


- 3 In the sidebar, click  **Coverage** to display the "Security coverage" view.



- 4 You can use the search bar to narrow down visible repositories in the "Security coverage" view based on name, or on the enablement status of security features.
- 5 In the list of repositories, select each repository you want to modify the enablement of security features for. To select all repositories on the page, click the checkbox next to **NUMBER Active**. To select all repositories that match the current search, click the checkbox next to **NUMBER Active** and then click **Select all NUMBER repos**.
- 6 Click **Security settings** next to **NUMBER selected**.
- 7 In the side panel, next to all the security features you want to enable or disable, select **Enable** or **Disable**.
- 8 As you make changes, the **Apply changes** button reports the number of security features you have edited. To confirm the changes, click **Apply changes NUMBER**. Alternatively, click **x** to close the panel without making changes.

Note: Enabling code scanning for multiple repositories in an organization using security overview will override any existing code scanning configurations for the selected repositories, including any previous query suite selections and workflows for advanced setups.



The security features that you can enable and disable in this view are:

- Dependency graph
- Dependabot alerts
- Dependabot security updates
- GitHub Advanced Security
- Code scanning default setup
- Secret scanning alerts
- Secret scanning as a push protection

If you're blocked from enabling a security feature due to an enterprise policy, you will still be able to see the affected repository in the "Security Coverage" view and access the side panel from the **Security settings** button. However, you will see a message in the side panel indicating that the functionality is not available. For more information about enterprise policies, see "[Enforcing policies for code security and analysis for your enterprise](#)."

Organization owners and security managers can use security overview to enable or disable security features for all repositories belonging to their organization. There are no enterprise policies that restrict organization owners or security managers from enabling or disabling any security features. For more information about enterprise policies, see "[About enterprise policies](#)."

Legal