Configuring default setup for code scanning at scale

In this article

You can quickly configure code scanning for repositories across your organization using default setup.

Code scanning is available for all public repositories on GitHub.com. To use code scanning in a private repository owned by an organization, you must have a license for GitHub Advanced Security. For more information, see "About GitHub Advanced Security."

About configuring default setup at scale

With default setup for code scanning, you can quickly secure code in repositories across your organization.

You can use the organization settings page labeled "Code security and analysis" to enable code scanning for all repositories in your organization that are eligible for default setup. For more information, see "Configuring default setup for all eligible repositories in an organization."

You can also use security overview to find a set of repositories in your organization and enable or disable default setup for all of them at the same time. For more information, see "Configuring default setup for a subset of repositories in an organization."

You can also create different default setup configurations for individual repositories. For more information on configuring default setup at the repository level, see "Configuring default setup for code scanning."

For repositories that are not eligible for default setup, you can configure advanced setup at the repository level, or at the organization level using a script. For more information, see "Configuring advanced setup for code scanning with CodeQL at scale."

Eligible repositories for CodeQL default setup at scale

A repository must meet all the following criteria to be eligible for default setup, otherwise you need to use advanced setup.

- Code scanning is not already enabled.
- GitHub Actions are enabled.
- Uses any CodeQL-supported language.
- Publicly visible, or GitHub Advanced Security is enabled.

About adding languages to an existing default setup configuration

If the code in a repository changes to include a CodeQL-supported language, GitHub will automatically update the code scanning configuration to include the new language. If code scanning fails with the new configuration, GitHub will resume the previous configuration automatically so the repository does not lose code scanning coverage.

Configuring default setup for all eligible repositories in an organization

Through the "Code security and analysis" page of your organization's settings, you can enable default setup for all eligible repositories in your organization. For more information on repository eligibility, see "Eligible repositories for CodeQL default setup at scale."

1. Click your profile photo, then click **Organizations**.
2. Click **Settings** next to your organization.
3. Click **Code security & analysis**.
4. Click **Enable all** next to "Code scanning".
5. In the "Query suites" section of the "Enable code scanning default setup" dialog box displayed, select the query suite your configuration of default setup will run. For more information, see "Built-in CodeQL query suites."
6. To enable your configuration of default setup, click **Enable for eligible repositories**.
7. Optionally, to recommend the "Extended" query suite throughout your organization when enabling default setup, select "Recommend the extended query suite for repositories enabling default setup."

Notes:

- If you disable CodeQL code scanning for all repositories this change is not reflected in the coverage information shown in security overview for the organization. The repositories will still appear to have code scanning enabled in the "Security Coverage" view.
- Enabling code scanning for all eligible repositories in an organization will not override existing code scanning configurations. For information on configuring default setup with different settings for specific repositories, see "Configuring default setup for code scanning" and "Configuring default setup for a subset of repositories in an organization."

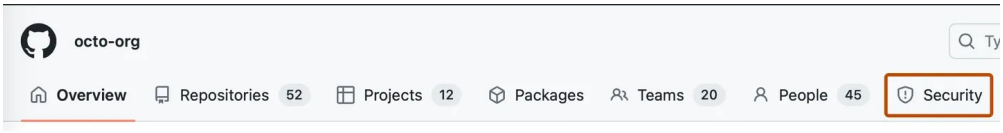
Configuring default setup for a subset of repositories in an organization

Through security overview for your organization, you can find eligible repositories for default setup, then enable default setup across each of those repositories simultaneously. For more information on repository eligibility, see "Eligible repositories for CodeQL default setup at scale."

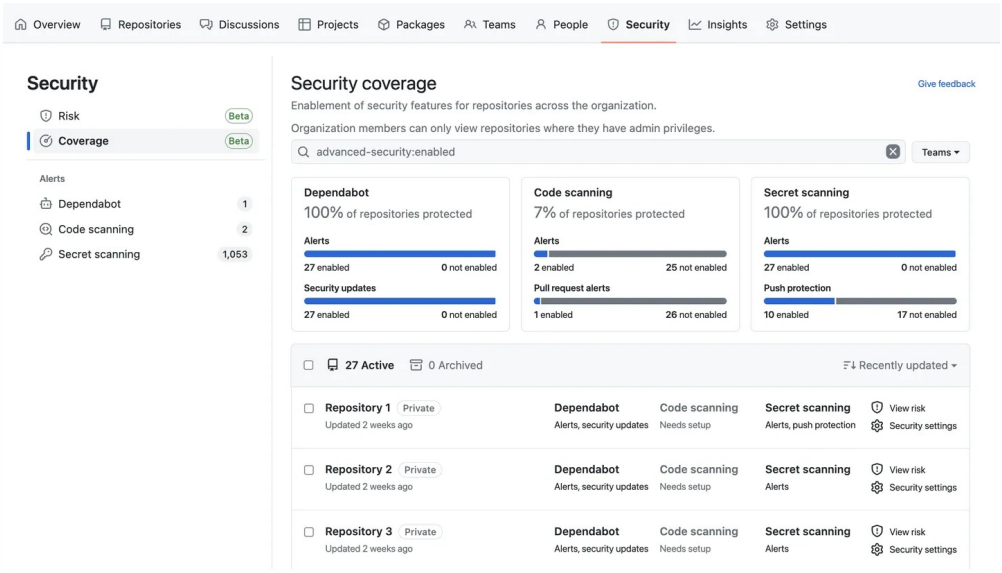
Finding repositories that are eligible for default setup

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.



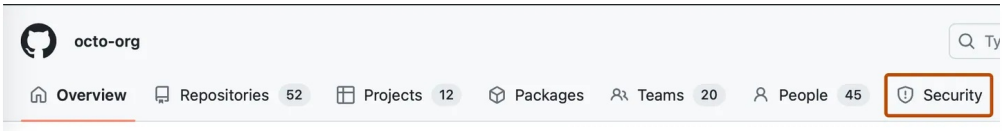
4. In the search bar, enter one of the following queries:

   - `code-scanning-default-setup:eligible is:public` shows repositories that have languages suitable for default setup and are eligible because they are visible to the public.
   - `code-scanning-default-setup:eligible advanced-security:enabled` shows private or internal repositories that have languages suitable for default setup and are eligible because they have GitHub Advanced Security enabled.
   - `code-scanning-default-setup:eligible is:private,internal advanced-security:not-enabled` shows private or internal repositories that have languages suitable for default setup but do not have GitHub Advanced Security enabled. Once you enable GitHub Advanced Security for these repositories, they can also be added to default setup.
   - `code-scanning-default-setup:not-eligible` shows repositories that either have advanced setup configured already, or where the languages not are suitable for default setup.

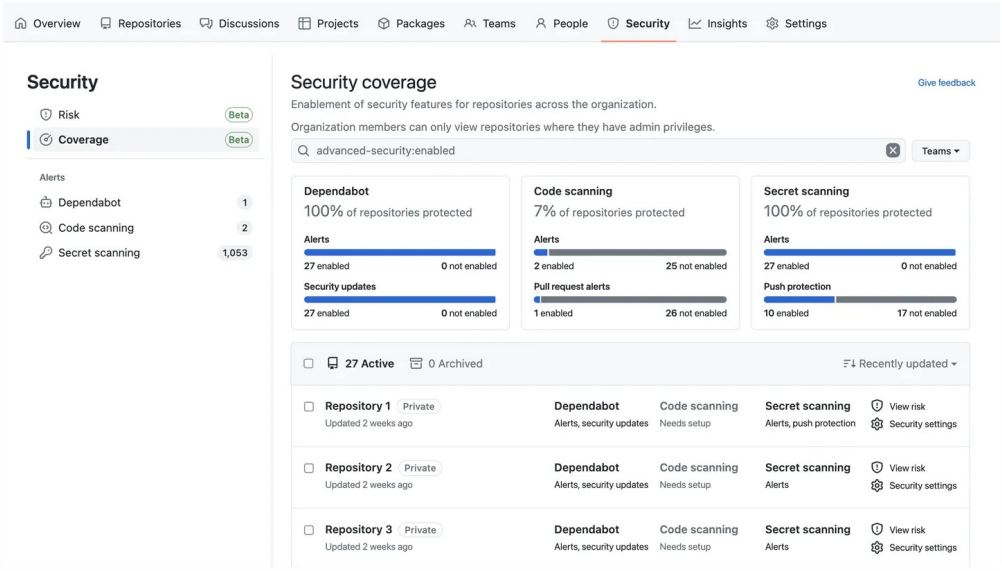
You can select all of the displayed repositories, or a subset of them, and enable or disable default setup for code scanning for them all at the same time. For more information, see step 5 of "Configuring default setup at scale for multiple repositories in an organization."

Configuring default setup at scale for multiple repositories in an organization

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. For example, to filter for repositories that are eligible for default setup and do not currently have default setup enabled, search for `code-scanning-default-setup:eligible`.

5. In the list of repositories, select each repository you want to enable code scanning 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**.

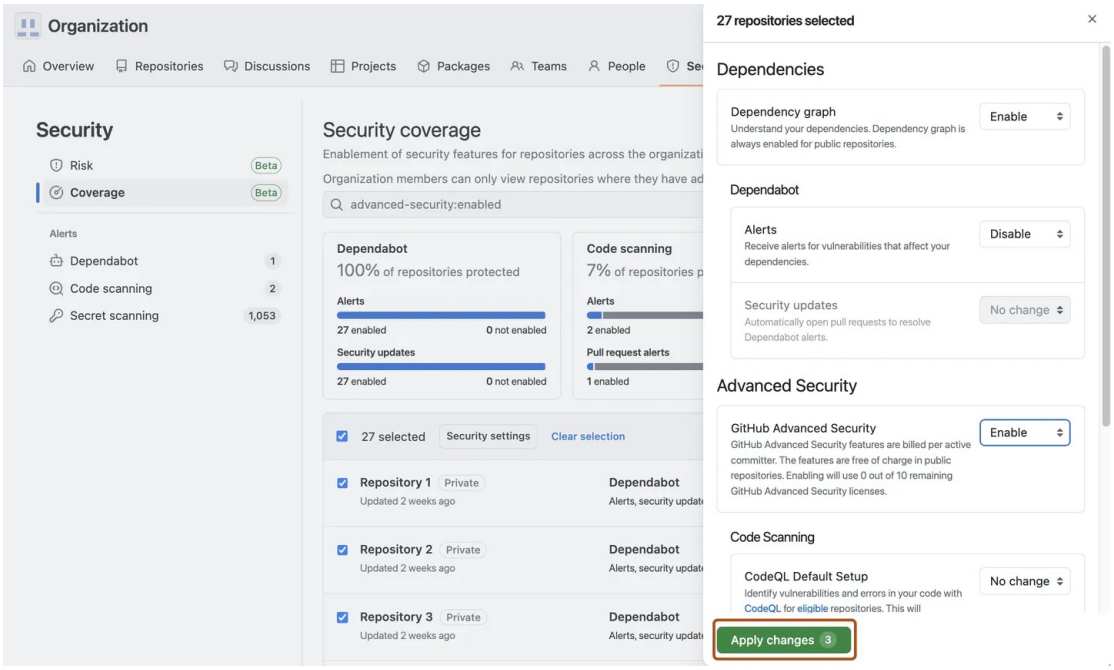
6. Click **Security settings** next to **NUMBER selected**.

7. In the side panel, in the "CodeQL Default Setup" section, select **No change**, then click **Enable**.

8. Optionally, to choose a different query suite than your organization's default query suite, select **Query suite: SUITE NAME**, then click the query suite your configuration of default setup should use. For more information, see "Built-in CodeQL query suites."

9. To confirm the enablement of code scanning for the selected repositories, click **Apply changes NUMBER**. Alternatively, to select or deselect more repositories for code scanning enablement, click × to close the panel without applying your 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.



If you're blocked from enabling code scanning 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 you cannot enable code scanning for the selected repositories. For more information about enterprise policies, see "Enforcing policies for code security and analysis for your enterprise."