Managing GitHub Advanced Security features for your enterprise

In this article

You can control GitHub Advanced Security features that secure and analyze code across all organizations owned by your enterprise.

> **Who can use this feature**
> Enterprise owners can manage Advanced Security features for organizations in an enterprise.

About management of Advanced Security features

You can use Advanced Security features to harden security for the organizations in your enterprise. To streamline management of Advanced Security, you can enable or disable each feature for all existing and/or new repositories within the organizations owned by your enterprise.

You can also enable or disable Advanced Security features via the API. For more information, see "Secret scanning" in the REST API documentation.

For information about buying a license for GitHub Advanced Security, see "Signing up for GitHub Advanced Security."

If you have disallowed GitHub Advanced Security for an organization, that organization will not be affected by enabling a feature for all existing repositories or for all new repositories. For more information about disallowing GitHub Advanced Security for an organization, see "Enforcing policies for code security and analysis for your enterprise."

When you enable one or more security and analysis features for existing repositories, you will see any results displayed on GitHub within minutes.

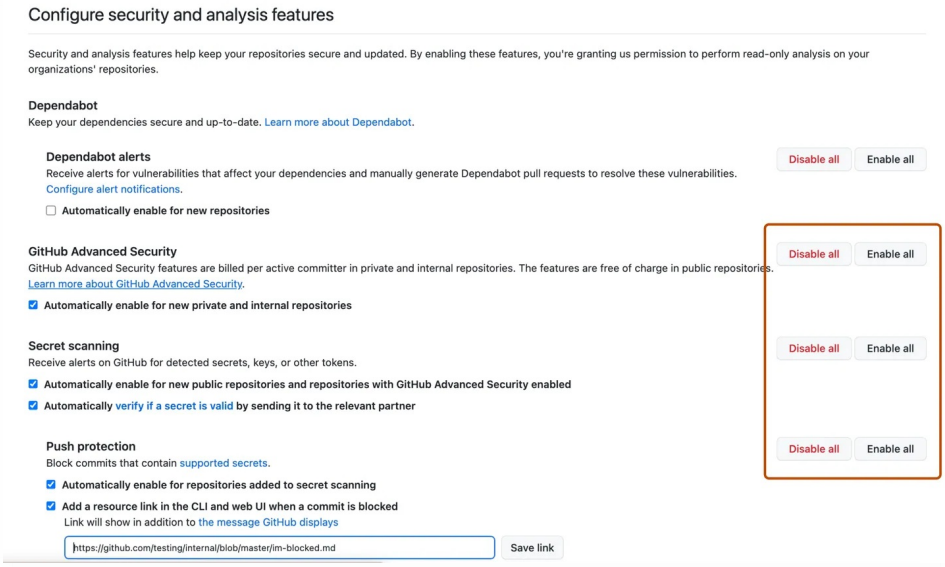
If you enable security and analysis features, GitHub performs read-only analysis on your repository.

Managing Advanced Security features

Note: If you enable GitHub Advanced Security, active committers to these repositories will use GitHub Advanced Security licenses. This option is deactivated if you have exceeded your license capacity. For more information, see "About billing for GitHub Advanced Security."

1. In the top-right corner of GitHub.com, click your profile photo, then click **Your enterprises**.
2. In the list of enterprises, click the enterprise you want to view.

3. In the enterprise account sidebar, click ⚙ **Settings**.
4. In the left sidebar, click **Code security & analysis**.
5. Optionally, enable or disable a feature for all existing repositories.
    - To the right of the feature, click **Disable all** or **Enable all**. If the control for "GitHub Advanced Security" is disabled, you have no available licenses for GitHub Advanced Security.



    - To confirm the change, click the **Enable/Disable all** or **Enable/Disable for eligible repositories** button in the dialog that is displayed.

6. Optionally, to enable or disable a feature automatically when new repositories are added, select the checkbox below the feature.
7. Optionally, to automatically allow secret scanning to check the validity of a secret by sending it to the relevant partner, select the relevant checkbox under "Secret scanning". You can also enable the validity check for a single repository or organization. For more information, see "Allowing validity checks for partner patterns in a repository," and "Allowing validity checks for partner patterns in an organization."

    > **Note:** Validity checks for partner patterns is currently in beta and subject to change.

8. Optionally, to include a resource link in the message that members will see when they attempt to push a secret, select **Add a resource link in the CLI and web UI when a commit is blocked**, then type a URL, and click **Save link**.

> **Note**: When a custom link is configured for an organization, the organization-level value overrides the custom link set for the enterprise. For more information, see "Push protection for repositories and organizations."