About GitHub Advanced Security

In this article

GitHub makes extra security features available to customers under an Advanced Security license. These features are also enabled for public repositories on GitHub.com.

GitHub Advanced Security is available for enterprise accounts on GitHub Enterprise Cloud and GitHub Enterprise Server. Some features of GitHub Advanced Security are also available for public repositories on GitHub.com. For more information, see "GitHub's plans."

For information about GitHub Advanced Security for Azure DevOps, see Configure GitHub Advanced Security for Azure DevOps in Microsoft Learn.

About GitHub Advanced Security

GitHub has many features that help you improve and maintain the quality of your code. Some of these are included in all plans, such as dependency graph and Dependabot alerts. Other security features require a GitHub Advanced Security (GHAS) license to run on repositories apart from public repositories on GitHub.com.

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

For information about how you can try GitHub Advanced Security for free, see "Setting up a trial of GitHub Advanced Security."

Note: If you want to use GitHub Advanced Security with Azure Repos, see GitHub Advanced Security & Azure DevOps in our resources site. For documentation, see Configure GitHub Advanced Security for Azure DevOps in Microsoft Learn.

About Advanced Security features

A GitHub Advanced Security license provides the following additional features:

- **Code scanning** - Search for potential security vulnerabilities and coding errors in your code. For more information, see "About code scanning."
- **Secret scanning** - Detect secrets, for example keys and tokens, that have been checked into the repository. If push protection is enabled, also detects secrets when

they are pushed to your repository. For more information, see "About secret scanning" and "Push protection for repositories and organizations."

- **Dependency review** - Show the full impact of changes to dependencies and see details of any vulnerable versions before you merge a pull request. For more information, see "About dependency review."

The table below summarizes the availability of GitHub Advanced Security features for public and private repositories.

	Public repository	Private repository without Advanced Security	Private repository with Advanced Security
Code scanning	✓	×	✓
Secret scanning	✓	×	✓
Dependency review	✓	×	✓

For information about Advanced Security features that are in development, see "GitHub public roadmap." For an overview of all security features, see "GitHub security features."

GitHub Advanced Security features are enabled for all public repositories on GitHub.com. Organizations that use GitHub Enterprise Cloud with Advanced Security can additionally enable these features for private and internal repositories.

Deploying GitHub Advanced Security in your enterprise

To learn about what you need to know to plan your GitHub Advanced Security deployment at a high level and to review the rollout phases we recommended, see "Adopting GitHub Advanced Security at scale."

Enabling Advanced Security features

For public repositories these features are permanently on and can only be disabled if you change the visibility of the project so that the code is no longer public.

For other repositories, once you have a license for your enterprise account, you can enable and disable these features at the organization or repository level. For more information, see "Managing security and analysis settings for your organization" and "Managing security and analysis settings for your repository."

If you have an enterprise account, license use for the entire enterprise is shown on your enterprise license page. For more information, see "Viewing your GitHub Advanced Security usage."

About starter workflows for Advanced Security

> **Note:** Starter workflows for Advanced Security have been consolidated in a "Security" category in the **Actions** tab of a repository. This new configuration is currently in beta and subject to change.

GitHub Enterprise Cloud provides starter workflows for security features such as code scanning. You can use these suggested workflows to construct your code scanning workflows, instead of starting from scratch.

For more information on starter workflows, see "Configuring advanced setup for code scanning" and "Using starter workflows."

Further reading

- "Enforcing policies for code security and analysis for your enterprise"