About billing for GitHub Advanced Security

In this article

If you want to use GitHub Advanced Security features, you need a license.

GitHub Advanced Security is available for enterprise accounts on GitHub Enterprise Cloud and GitHub Enterprise Server. 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 billing for GitHub Advanced Security

You can make extra features for code security available to users by buying and uploading a license for GitHub Advanced Security. For more information about GitHub Advanced Security, see "About GitHub Advanced Security."

Each license for GitHub Advanced Security specifies a maximum number of accounts that can use these features. Each active committer to at least one repository with the feature enabled uses one license. A committer is considered active if one of their commits has been pushed to the repository within the last 90 days, regardless of when it was originally authored.

Note: Active committers are calculated using both the commit author information and the timestamp for when the code was pushed to GitHub Enterprise Server.

- When a user pushes code to GitHub, every user who authored code in that push counts towards GitHub Advanced Security licenses, even if the code is not new to GitHub.
- Users should always create branches from a recent base, or rebase them before pushing. This will ensure that users who have not committed in the last 90 days do not take up GitHub Advanced Security licenses.

You can determine how many licenses you'll need for GitHub Advanced Security by generating a count of your instance's active committers in the site admin dashboard. For more information, see "Site admin dashboard."

About committer numbers for GitHub Advanced Security

We record and display two numbers of active committers for GitHub Advanced Security on your GitHub Enterprise Server instance:

- **Active committers** is the number of committers who contributed to at least one repository in an organization and who use a license in your enterprise. That is, they are also an organization member, an external collaborator, or have a pending invitation to join an organization in your enterprise, and they are not a GitHub App bot. For information about differences between bot and machine accounts, see "Differences between GitHub Apps and OAuth apps."
- **Unique to this repository/organization** is the number of active committers who contributed only to this repository, or to repositories in this organization. This number shows how many licenses you can free up by deactivating GitHub Advanced Security for that repository or organization.

If there are no unique active committers, all active committers also contribute to other repositories or organizations that use GitHub Advanced Security. Deactivating the feature for that repository or organization would not free any licenses for GitHub Advanced Security.

When you remove a user from your enterprise account, the user's license is freed within 24 hours.

> **Note:** Users can contribute to multiple repositories or organizations. Usage is measured across the whole enterprise account to ensure that each member uses one license regardless of how many repositories or organizations the user contributes to.

When you activate or deactivate Advanced Security for repositories, GitHub displays an overview of changes to the use of your license. If you deactivate access to GitHub Advanced Security, any licenses used by unique active committers are freed up.

If you are over your license limit, GitHub Advanced Security continues to work on all repositories where it is already enabled. However, in organizations where GitHub Advanced Security is enabled for new repositories, repositories will be created with the feature deactivated. In addition, the option to enable GitHub Advanced Security for existing repositories will not be available.

As soon as you free up some licenses, by deactivating GitHub Advanced Security for some repositories or by increasing your license size, the options for activating GitHub Advanced Security will work again as normal.

You can enforce policies to allow or disallow the use of Advanced Security by organizations owned by your enterprise account. For more information, see "Enforcing policies for Advanced Security in your enterprise."

For more information on viewing license usage, see "Viewing your GitHub Advanced Security usage."

Understanding active committer usage

The following example timeline demonstrates how active committer count for GitHub Advanced Security could change over time in an enterprise. For each month, you will find events, along with the resulting committer count.

Date	Events during the month	Total committers
April 15	A member of your enterprise enables GitHub Advanced Security for repository **X**. Repository **X** has 50 committers over the past 90 days.	**50**

May 1	Developer **A** leaves the team working on repository **X**. Developer **A**'s contributions continue to count for 90 days.	**50**
August 1	Developer **A**'s contributions no longer count towards the licenses required, because 90 days have passed.	50 - 1 = **49**
August 15	A member of your enterprise enables GitHub Advanced Security for a second repository, repository **Y**. In the last 90 days, a total of 20 developers contributed to that repository. Of those 20 developers, 10 also recently worked on repo **X** and do not require additional licenses.	49 + 10 = **59**
August 16	A member of your enterprise disables GitHub Advanced Security for repository **X**. Of the 49 developers who were working on repository **X**, 10 still also work on repository **Y**, which has a total of 20 developers contributing in the last 90 days.	49 - 29 = **20**

Note: A user will be flagged as active when their commits are pushed to any branch of a repository, even if the commits were authored more than 90 days ago.

Getting the most out of GitHub Advanced Security

When you decide which repositories and organizations to prioritize for GitHub Advanced Security, you should review them and identify:

- Codebases that are the most critical to your company's success. These are the projects for which the introduction of vulnerable code, hard-coded secrets, or insecure dependencies would have the greatest impact on your company.
- Codebases with the highest commit frequency. These are the most actively developed projects, consequently there is a higher risk that security problems could be introduced.

When you have enabled GitHub Advanced Security for these organizations or repositories, assess which other codebases you could add without incurring billing for unique active committers. Finally, review the remaining important and busy codebases. If you want to increase the number of licensed active committers, contact GitHub's Sales team.