Enforcing policies for code security and analysis for your enterprise

In this article

About policies for GitHub Advanced Security in your enterprise

Enforcing a policy for the use of GitHub Advanced Security in your enterprise's organizations

You can enforce policies to manage the use of GitHub Advanced Security features within your enterprise's organizations.

> **Who can use this feature**
> Enterprise owners can enforce policies for GitHub Advanced Security in an enterprise.

> GitHub Advanced Security is available for enterprise accounts on GitHub Enterprise Cloud and GitHub Enterprise Server. For more information, see "[GitHub's products]()."
>
> For information about GitHub Advanced Security for Azure DevOps, see [Configure GitHub Advanced Security for Azure DevOps]() in Microsoft Learn.

About policies for GitHub Advanced Security in your enterprise 🔗

GitHub Advanced Security helps developers improve and maintain the security and quality of code. For more information, see "[About GitHub Advanced Security]()." For more information, see "[About GitHub Advanced Security]()."

If you purchase a license for GitHub Advanced Security, any organization on your GitHub Enterprise Server instance can use Advanced Security features. You can enforce policies to control how members of your enterprise on GitHub Enterprise Server use Advanced Security.

## Enforcing a policy for the use of GitHub Advanced Security in your enterprise's organizations 🔗

GitHub bills for Advanced Security on a per-committer basis. For more information, see "[Managing billing for GitHub Advanced Security]()."

You can enforce a policy that controls whether repository administrators are allowed to enable features for Advanced Security in an organization's repositories. You can configure a policy for all organizations owned by your enterprise account, or for individual organizations that you choose.

Disallowing Advanced Security for an organization prevents repository administrators from enabling Advanced Security features for additional repositories, but does not disable the features for repositories where the features are already enabled. For more information about configuration of Advanced Security features, see "Managing security and analysis settings for your organization" or "Managing security and analysis settings for your repository."

> **Note:** This policy only impacts repository administrators, specifically. Organization owners and security managers can always enable security features, regardless of how you set this policy. For more information, see "Roles in an organization."

1. In the top-right corner of GitHub Enterprise Server, click your profile photo, then click **Enterprise settings**.
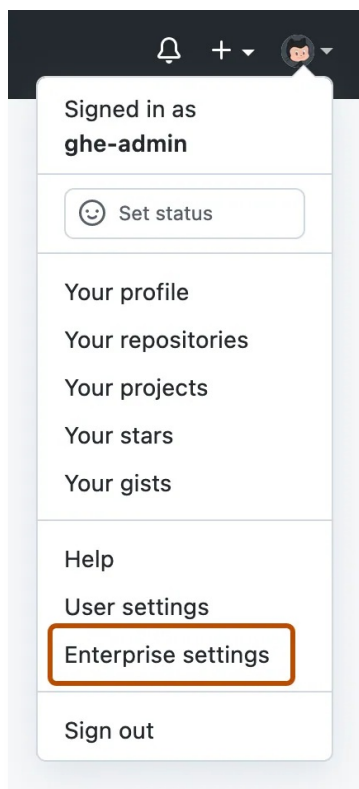
2. In the enterprise account sidebar, click ⚖ **Policies**.

3. Under ⚖ "Policies", click **Advanced Security**.

4. Optionally, if you chose **Allow for selected organizations**, to the right of an organization, select the dropdown menu to enable Advanced Security for the organization.

GitHub Advanced Security availability

If allowed, organizations can enable GitHub Advanced Security. If not allowed, organizations cannot enable GitHub Advanced Security. Note: changing this setting does not enable/disable GitHub Advanced Security for repositories in selected organizations.

Allow for selected organizations ▾

🔍 Filter organizations

☐ Select organizations (0)	
☐ ▨ a-fun-new-org	Available ▾

   ✓ **Available**
     GitHub Advanced Security is available for all repositories within this organization.

   Not available
     GitHub Advanced Security won't be available for repositories within this organization.

☐ ▨ A1EBD7CC0EB3	
☐ ▨ AADTestScim	
☐ ▨ aashijtestorg	Not available ▾