Enforcing policies for code security and analysis for your enterprise

In this article

About policies for code security and analysis in your enterprise

Enforcing a policy to manage the use of Dependabot alerts in your enterprise

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

Enforcing a policy to manage the use of GitHub Advanced Security features in your enterprise's repositories

Enforcing a policy to manage the use of secret scanning in your enterprise's repositories

You can enforce policies to manage the use of code security and analysis features within your enterprise's organizations.

> **Who can use this feature**
> Enterprise owners can enforce code security and analysis 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 plans."
>
> For information about GitHub Advanced Security for Azure DevOps, see Configure GitHub Advanced Security for Azure DevOps in Microsoft Learn.

About policies for code security and analysis in your enterprise 🔗

You can enforce policies to manage the use of code security and analysis features within organizations owned by your enterprise. You can allow or disallow people with admin access to a repository to enable or disable the security and analysis features.
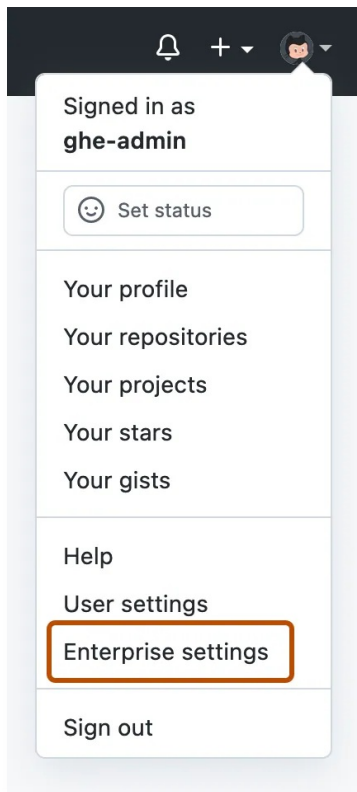
Additionally, you can enforce policies for the use of GitHub Advanced Security in your enterprise's organizations and repositories.

Enforcing a policy to manage the use of Dependabot alerts in your enterprise 🔗

Across all organizations owned by your enterprise, you can allow members with admin permissions for repositories to enable or disable Dependabot alerts and change Dependabot alerts settings.

> **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 **Code security and analysis**.

4. Under "Enable or disable Dependabot alerts by repository admins", use the dropdown menu to choose a policy.

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**.
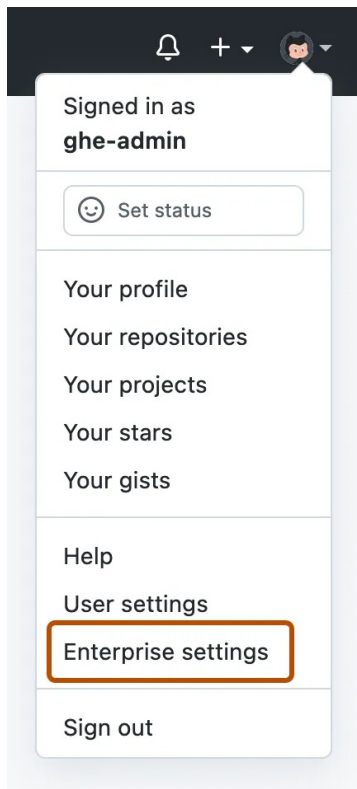
2 In the enterprise account sidebar, click ⚖ **Policies**.

3 Under ⚖ "Policies", click **Code security and analysis**.

4 In the "GitHub Advanced Security policies" section, under "GitHub Advanced Security availability", select the dropdown menu and click a policy for the organizations owned by your enterprise.

5 Under "GitHub Advanced Security availability", select the dropdown menu, then click a policy for the organizations owned by your enterprise.

6 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.

☐ 🟢 A1EBD7CC0EB3   **Not available**
                                      GitHub Advanced Security won't be
☐ 🟡 AADTestScim   available for repositories within this
                                      organization.

☐ 🔴 aashijtestorg   Not available ▾

Enforcing a policy to manage the use of GitHub Advanced Security features in your enterprise's repositories 🔗

Across all of your enterprise's organizations, you can allow or disallow people with admin access to repositories to manage the use of GitHub Advanced Security features in the repositories. GitHub Advanced Security features must be available to the organization for this policy to take effect. For more information, see "Enforcing a policy for the use of GitHub Advanced Security in your enterprise's organizations."

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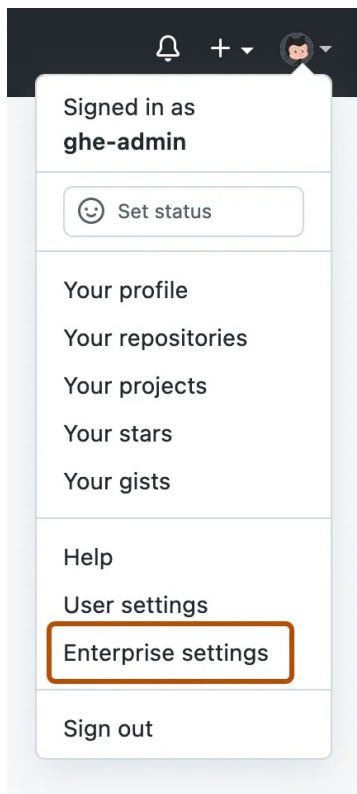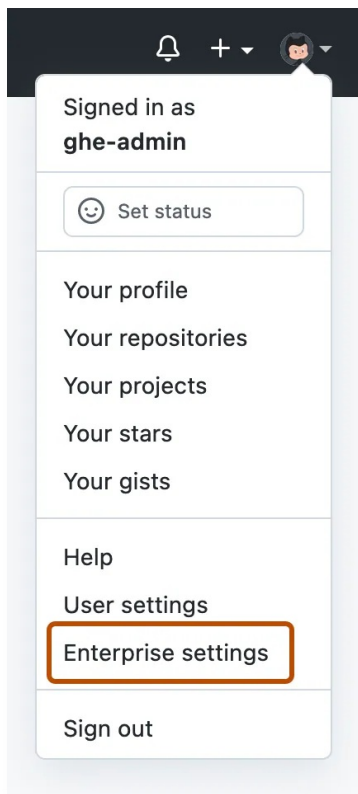
2 In the enterprise account sidebar, click ⚖ **Policies**.

3 Under ⚖ "Policies", click **Code security and analysis**.

4 In the "GitHub Advanced Security policies" section, under "Enable or disable GitHub Advanced Security by repository admins", select the dropdown menu and click a policy.

Enforcing a policy to manage the use of secret scanning in your enterprise's repositories 🔗

Across all of your enterprise's organizations, you can allow or disallow people with admin access to repositories to manage and configure secret scanning for the repositories. GitHub Advanced Security features must be available to the organization for this policy to take effect. For more information, see "Enforcing a policy for the use of GitHub Advanced Security in your enterprise's organizations."

> **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 **Code security and analysis**.

4 In the "GitHub Advanced Security policies" section, under "Enable or disable secret scanning by repository admins", select the dropdown menu and click a policy.