Enabling GitHub Advanced Security for your enterprise

In this article

You can configure GitHub Enterprise Server to include GitHub Advanced Security. This provides extra features that help users find and fix security problems in their code.

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 enabling GitHub Advanced Security

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

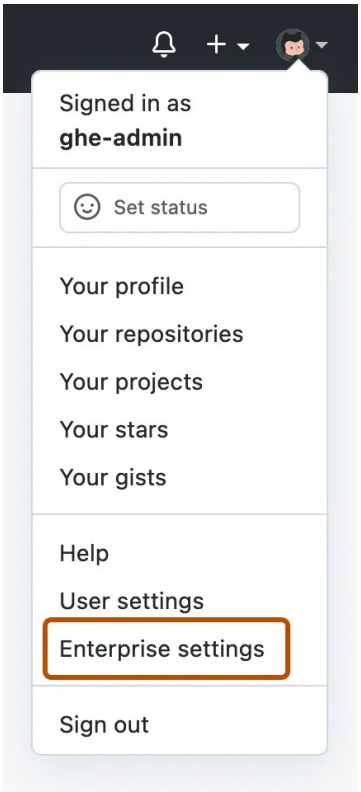
When you enable GitHub Advanced Security for your enterprise, repository administrators in all organizations can enable the features unless you set up a policy to restrict access. For more information, see "Enforcing policies for code security and analysis for your enterprise."

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

For guidance on a phased deployment of GitHub Advanced Security, see "Introduction to adopting GitHub Advanced Security at scale."

Checking whether your license includes GitHub Advanced Security

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 ⚙ **Settings**.
3. Under ⚙ **Settings**, click **License**.
4. If your license includes GitHub Advanced Security, the license page includes a section showing details of current usage.

Prerequisites for enabling GitHub Advanced Security

1. Upgrade your license for GitHub Enterprise Server to include GitHub Advanced Security. For information about licensing, see "About billing for GitHub Advanced Security."
2. Download the new license file. For more information, see "Downloading your license for GitHub Enterprise."
3. Upload the new license file to your GitHub Enterprise Server instance. For more information, see "Uploading a new license to GitHub Enterprise Server."
4. Review the prerequisites for the features you plan to enable.
   - Code scanning, see "Configuring code scanning for your appliance."
   - Secret scanning, see "Configuring secret scanning for your appliance."
   - Dependabot, see "Enabling Dependabot for your enterprise."

Enabling and disabling GitHub Advanced Security features

Warning: Changing this setting will cause user-facing services on GitHub Enterprise Server to

restart. You should time this change carefully, to minimize downtime for users.

1. From an administrative account on GitHub Enterprise Server, in the upper-right corner of any page, click 🚀.
2. If you're not already on the "Site admin" page, in the upper-left corner, click **Site admin**.
3. In the "🚀 Site admin" sidebar, click **Management Console**.
4. In the "Settings" sidebar, click **Security**.
5. Under "Security," select the features that you want to enable and deselect any features you want to disable.
6. Under the "Settings" sidebar, click **Save settings**.

   > **Note:** Saving settings in the Management Console restarts system services, which could result in user-visible downtime.

7. Wait for the configuration run to complete.

When GitHub Enterprise Server has finished restarting, you're ready to set up any additional resources required for newly enabled features. For more information, see "Configuring code scanning for your appliance."

Enabling or disabling GitHub Advanced Security features via the administrative shell (SSH)

You can enable or disable features programmatically on your GitHub Enterprise Server instance. For more information about the administrative shell and command-line utilities for GitHub Enterprise Server, see "Accessing the administrative shell (SSH)" and "Command-line utilities."

For example, you can enable any GitHub Advanced Security feature with your infrastructure-as-code tooling when you deploy an instance for staging or disaster recovery.

1. SSH into your GitHub Enterprise Server instance.
2. Enable features for GitHub Advanced Security.
   - To enable Code scanning, enter the following commands.

```
ghe-config app.minio.enabled true
ghe-config app.code-scanning.enabled true
```

   - To enable Secret scanning, enter the following command.

```
ghe-config app.secret-scanning.enabled true
```

   - To enable the dependency graph, enter the following command.

```
ghe-config app.dependency-graph.enabled true
```

3. Optionally, disable features for GitHub Advanced Security.
   - To disable code scanning, enter the following commands.

```
ghe-config app.minio.enabled false
ghe-config app.code-scanning.enabled false
```

   - To disable secret scanning, enter the following command.

```
ghe-config app.secret-scanning.enabled false
```

   - To disable the dependency graph, enter the following command.

```
ghe-config app.dependency-graph.enabled false
```

4. Apply the configuration.

```
ghe-config-apply
```