About secret scanning

In this article

GitHub Enterprise Cloud scans repositories for known types of secrets, to prevent fraudulent use of secrets that were committed accidentally.

Secret scanning alerts for partners runs automatically on public repositories and public npm packages to notify service providers about leaked secrets on GitHub.com.
Secret scanning alerts for users are available for free on all public repositories. Organizations using GitHub Enterprise Cloud with a license for GitHub Advanced Security can also enable secret scanning alerts for users on their private and internal repositories. For more information, see "About secret scanning" and "About GitHub Advanced Security."
For information about how you can try GitHub Advanced Security for free, see "Setting up a trial of GitHub Advanced Security."

About secret scanning

If your project communicates with an external service, you might use a token or private key for authentication. Tokens and private keys are examples of secrets that a service provider can issue. If you check a secret into a repository, anyone who has read access to the repository can use the secret to access the external service with your privileges. We recommend that you store secrets in a dedicated, secure location outside of the repository for your project.

Secret scanning will scan your entire Git history on all branches present in your GitHub repository for secrets, even if the repository is archived. Secret scanning also searches issue descriptions and comments for secrets.

Additionally, secret scanning scans the titles, descriptions, and comments, in open and closed historical issues, and reports leaked secrets as alerts on GitHub. A notification is sent to the relevant partner when a historical partner pattern is detected.

Secret scanning is available on GitHub.com in two forms:

1. **Secret scanning alerts for partners.** Runs automatically on all public repositories and public npm packages. Service providers can partner with GitHub to provide their secret formats for scanning, hence the term "partners." To find out about our partner program, see "Secret scanning partner program." Any strings that match patterns that were provided by secret scanning partners are reported directly to the relevant partner. For more information, see the "About secret scanning alerts for partners" section below.
2. **Secret scanning alerts for users.** You can enable and configure additional

scanning for repositories owned by organizations that use GitHub Enterprise Cloud for any public repositories (for free), and for private and internal repositorites when you have a license for GitHub Advanced Security.

Any strings that match patterns provided by secret scanning partners, by other service providers, or defined by you or your organization, are reported as alerts in the **Security** tab of repositories. If a string in a public repository matches a partner pattern, it is also reported to the partner. For more information, see the "About secret scanning alerts for users" section below.

You can audit the actions taken in response to secret scanning alerts using GitHub tools. For more information, see "Auditing security alerts."

You can also enable secret scanning as a push protection for a repository or an organization. When you enable this feature, secret scanning prevents contributors from pushing code with a detected secret. To proceed, contributors must either remove the secret(s) from the push or, if needed, bypass the protection. Admins can also specify a custom link that is displayed to the contributor when a push is blocked; the link can contain resources specific to the organization to aid contributors. For more information, see "Push protection for repositories and organizations."

Additionally, you can enable push protection for yourself, so that no matter which public repository you push to, you will be protected. For more information, see "Push protection for users."

Note: When you fork a repository with secret scanning or push protection enabled, these features are not enabled by default on the fork. You can enable secret scanning or push protection on the fork the same way you enable them on a standalone repository.

About secret scanning alerts for partners

When you make a repository public, or push changes to a public repository, GitHub Enterprise Cloud always scans the code for secrets that match partner patterns. Public packages on the npm registry are also scanned. Secret scanning also searches issue descriptions and comments for secrets. If secret scanning detects a potential secret, we notify the service provider who issued the secret. The service provider validates the string and then decides whether they should revoke the secret, issue a new secret, or contact you directly. Their action will depend on the associated risks to you or them. For more information, see "Secret scanning patterns."

You cannot change the configuration of secret scanning for partner patterns on public repositories.

About secret scanning alerts for users

Secret scanning alerts for users are available for free on all public repositories, and for private and internal repositories that are owned by organizations using GitHub Enterprise Cloud with a license for GitHub Advanced Security. When you enable secret scanning for a repository, GitHub scans the code for patterns that match secrets used by many service providers. When the scan is completed, GitHub sends an email alert to the enterprise and organization owners, even if no secrets were found.

Secret scanning also searches issue descriptions and comments for secrets. When a supported secret is leaked, GitHub Enterprise Cloud generates a secret scanning alert. GitHub will also periodically run a full git history scan of existing content in GitHub Advanced Security repositories where secret scanning is enabled, and send alert notifications following the secret scanning alert notification settings. For more information, see "Supported secrets for user alerts."

If you're a repository administrator, you can enable secret scanning alerts for users for any repository, including archived repositories. Organization owners can also enable secret scanning alerts for users for all repositories or for all new repositories within an organization. For more information, see "Managing security and analysis settings for your repository" and "Managing security and analysis settings for your organization."

You can also define custom secret scanning patterns for a repository, organization, or enterprise. For more information, see "Defining custom patterns for secret scanning."

GitHub stores detected secrets using symmetric encryption, both in transit and at rest.

Accessing secret scanning alerts

When you enable secret scanning for a repository or push commits to a repository with secret scanning enabled, GitHub scans the contents for secrets that match patterns defined by service providers and any custom patterns defined in your enterprise, organization, or repository. Secret scanning also searches issue descriptions and comments for secrets. GitHub also runs a scan of all historical code content in repositories with secret scanning enabled when a new partner pattern or custom pattern is added or updated.

If secret scanning detects a secret in a commit, issue description, or comment, GitHub generates an alert.

- GitHub sends an email alert to the repository administrators and organization owners. You'll receive an alert if you are watching the repository, if you have enabled notifications either for security alerts or for all the activity on the repository, and if, in your notification settings, you have selected to receive email notifications for the repositories that you are watching.
- If the person who introduced the secret in the commit, issue description, or comment isn't ignoring the repository, GitHub will also send them an email alert. The emails contains a link to the related secret scanning alert. The person who introduced the secret can then view the alert in the repository, and resolve the alert.
- GitHub displays an alert in the **Security** tab of the repository.

For more information about viewing and resolving secret scanning alerts, see "Managing alerts from secret scanning."

For more information on how to configure notifications for secret scanning alerts, see "Configuring notifications for secret scanning alerts."

Repository administrators and organization owners can grant users and teams access to secret scanning alerts. For more information, see "Managing security and analysis settings for your repository."

You can use security overview to see an organization-level view of which repositories have enabled secret scanning and the alerts found. For more information, see "About security overview."

You can also use the REST API to monitor results from secret scanning across your repositories. For more information about API endpoints, see "Secret scanning."

Further reading

- "Securing your repository"
- "Keeping your account and data secure"
- "Best practices for preventing data leaks in your organization"
- "Managing secrets for your codespaces"
- "Configuring access to private registries for Dependabot"
- "Using secrets in GitHub Actions"