

# GitHub Integration - Elastic

## GitHub Integration

The GitHub integration collects events from the [GitHub API\(external, opens in a new tab or window\)](#).

### Logs

#### Audit

The GitHub audit log records all events related to the GitHub organization. See [Audit log actions\(external, opens in a new tab or window\)](#) for more details.

To use this integration, the following prerequisites must be met:

- You must be an organization owner.
- You must be using Github Enterprise Cloud.
- You must use a Personal Access Token with `read:audit_log` scope.

*This integration is not compatible with GitHub Enterprise server.*

### Code Scanning

The Code Scanning lets you retrieve all security vulnerabilities and coding errors from a repository setup using Github Advanced Security Code Scanning feature. See [About code scanning\(external, opens in a new tab or window\)](#) for more details.

To use this integration, GitHub Apps must have the `security_events` read permission. Or use a personal access token with the `security_events` scope for private repos or `public_repo` scope for public repos. See [List code scanning alerts\(external, opens in a new tab or window\)](#)

### Secret Scanning

The Github Secret Scanning lets you retrieve secret scanning for advanced security alerts from a repository setup using Github Advanced Security Secret Scanning feature. See [About Secret scanning\(external, opens in a new tab or window\)](#) for more details.

To use this integration, GitHub Apps must have the `secret_scanning_alerts` read permission. Or you must be an administrator for the repository or for the organization that owns the repository, and you must use a personal access token with the `repo` scope or `security_events` scope. For public repositories, you may instead use the `public_repo` scope. See [List secret scanning alerts](#)

## Dependabot

The Github Dependabot lets you retrieve known vulnerabilities in dependencies from a repository setup using Github Advanced Security Dependabot feature. See [About Dependabot\(external, opens in a new tab or window\)](#) for more details.

To use this integration, you must be an administrator for the repository or for the organization that owns the repository, and you must use a personal access token with the `repo` scope or `security_events` scope. For public repositories, you may instead use the `public_repo` scope. See [Authenticating with GraphQL\(external, opens in a new tab or window\)](#) and [Token Issue\(external, opens in a new tab or window\)](#)

## Issues

The Github Issues datastream lets you retrieve github issues, including pull requests, issue assignees, comments, labels, and milestones. See [About Issues\(external, opens in a new tab or window\)](#) for more details. You can retrieve issues for specific repository or for entire organization. Since Github API considers pull requests as issues, users can use `github.issues.is_pr` field to filter for only pull requests.

All issues including `closed` are retrieved by default. If users want to retrieve only `open` requests, you need to change `State` parameter to `open`.

To use this integration, users must use Github Apps or Personal Access Token with `read` permission to repositories or organization. Please refer to [Github Apps Permissions Required\(external, opens in a new tab or window\)](#) and [Personal Access Token Permissions Required\(external, opens in a new tab or window\)](#) for more details.

---

Revision #1

Created 23 April 2025 21:14:22 by Richmond Abella

Updated 23 April 2025 21:18:48 by Richmond Abella