opentext™

OpenText™ Fortify GitHub Integration Guide

Document Release Date: August 2024

Fortify AST Scan

The Fortify AST Scan Action adds application security testing (AST) to your GitHub repositories. This action includes the tasks in the following table.

Task	More information
Submit a static application security testing (SAST) scan request and optional Software Composition Analysis scan request to Fortify on Demand.	"Setting up a Fortify on Demand SAST scan" on the next page
Submit a SAST scan request to Fortify ScanCentral SAST.	"Setting up a Fortify ScanCentral SAST scan" on page 5

This document provides instructions on using the action. This document assumes that you have a working knowledge of GitHub Actions.

This section covers the following topics:

Fortify AST Scan prerequisites

The following prerequisites must be met to use the Fortify AST Scan Action:

- Enable GitHub Actions in the repository or the organization.
- Have at least one runner available for the repository. If you are using self-hosted runners, make sure they include the necessary software to run the action. For more information, see the action documentation.

Setting up a Fortify on Demand SAST scan

To set up an action to run a Fortify on Demand SAST scan:

1. Configure static scan settings in Fortify on Demand. For instructions, see the Fortify on Demand documentation.

   Note: It is not necessary to prepare your application's source code in advance, as the action invokes the Fortify ScanCentral SAST client to package your application. Fortify ScanCentral SAST supports the following languages: .NET and .NET Core (MSBuild projects), Apex, Classic ASP, ColdFusion, IaC files, Go, Java (Gradle and Maven projects), JavaScript/TypeScript, Kotlin for Android, PHP, Python, and Ruby.

   If you are using self-hosted runners, make sure they meet the requirements for the specified Fortify ScanCentral SAST client version. See Fortify Software System Requirements.

2. Create repository secrets in GitHub to store sensitive information, such as credentials. For more information on creating secrets, see the GitHub Actions documentation.

   The following table lists the repository secrets. You can customize Name values.

Name	Description	Notes
FOD_CLIENT_ID	API key	Use either API credentials (key and secret) or user credentials (username, PAT, tenant code). For instructions on creating an API key or personal access token, see the Fortify on Demand documentation.
FOD_CLIENT_SECRET	API secret	
FOD_USER	Username	
FOD_PAT	OpenText strongly recommends using a personal access token (PAT). The PAT must have the following scope: `api-tenant`	
FOD_TENANT	Tenant code	

3. Create a `fortify.yml` file in the `.github/workflows` directory in the repository.
4. In the `fortify.yml` file, add the workflow for the Fortify AST Scan Action. The starter workflow provides a template to package the source code, submit a scan request, and optionally export scan results to the GitHub Security view of the repository.
5. Customize the workflow. Make sure to specify relevant triggering events and environment variables:
   - Review the triggering events available on GitHub Actions to choose onesthat align with your development needs. Commonly used event triggers include pull request against default branch, push to default branch, and weekly scheduled scanning.
   - Specify the Fortify on Demand environment variables listed in the following table. For more information about these variables, see the action documentation.

Name	Required	Description
FOD_URL	Yes	Domain URL
FOD_CLIENT_ID	Yes	GitHub context: `${{secrets.<FOD_CLIENT_ID>}}` **Note:** Use either API credentials (key and secret) or user credentials (username, PAT, tenant code)
FOD_CLIENT_SECRET	Yes	GitHub context: `${{secrets.<FOD_CLIENT_SECRET>}}`
FOD_USER	Yes	GitHub context: `${{secrets.<FOD_USER>}}` **Note:** Use either API credentials (key and secret) or user credentials (username, PAT, tenant code)
FOD_PASSWORD	Yes	GitHub context: `${{secrets.<FOD_PAT>}}`
FOD_TENANT	Yes	GitHub context: `${{secrets.<FOD_TENANT>}}`

Name	Required	Description
FOD_RELEASE	No	Release identifier as one of the following: ◦ Numeric release ID ◦ *<app_name>:<release_name>* ◦ *<app_name>:<microservice_name>:<release_name>* (for microservices applications) The default value is: `<github.repository>:<github.head_ref || github.ref_name>`, for example, `myOrg/myRepo:myBranch`.
EXTRA_FOD_LOGIN_OPTS	No	Specify additional Fortify on Demand login options.
EXTRA_PACKAGE_OPTS	No	Specify additional Fortify ScanCentral SAST packaging options. For more information on the packaging options, see the Fortify ScanCentral SAST Installation, Configuration, and Usage Guide. If you want to include an OpenText™ Debricked Software Composition Analysis scan, make sure to specify `-oss`. For the list of Debricked-supported languages, see Language Support.
EXTRA_FOD_SAST_SCAN_OPTS	No	Specify additional SAST scan options.
DO_WAIT	No	Set to `true` to have the action poll Fortify on Demand for SAST scan completion.
DO_EXPORT	No	Set to `true` to export scan results to the GitHub Security view of the repository. Polling for scan completion is included.
TOOL_DEFINITIONS	No	Specify tool definitions.

6. Commit your changes made to the workflow.

Setting up a Fortify ScanCentral SAST scan

The Fortify ScanCentral SAST Controller must be accessible from the GitHub runner where your workflow runs.

To set up an action to perform a Fortify ScanCentral SAST scan:

1. Create repository secrets in GitHub to store sensitive information. For more information about creating secrets, see the GitHub Actions documentation.

   The following table lists the repository secrets for a Fortify ScanCentral SAST scan.

Name	Description	Notes
SC_SAST_TOKEN	Client authentication token to connect to the Controller	
SSC_URL	Fortify Software Security Center URL	This Fortify Software Security Center instance must be associated with a Fortify ScanCentral SAST Controller
SSC_TOKEN	A Fortify Software Security Center authentication token of type CIToken	Use either a token or user account credentials (user name and password).
SSC_USER	Fortify Software Security Center user name	
SSC_PASSWORD	Fortify Software Security Center password	

2. Create a `fortify.yml` file in the `.github/workflows` directory in the repository and add the workflow for the Fortify AST Scan Action.

   The starter workflow provides a template to package the source, initiate a scan, and optionally export analysis results to the GitHub Security view of the repository.

3. Configure the events to trigger the workflow and customize environment variables.

   Commonly used event triggers include pull request against a default branch, push to a default branch, and weekly scheduled scanning.

   The following table describes the available environment variables for a Fortify ScanCentral

SAST scan. For more information about these variables, see the action documentation.

Name	Required	Description
SC_SAST_SENSOR_VERSION	Yes	Specify the version (*<year>.<quarter>*) of the Fortify ScanCentral SAST sensor to perform the scan.
EXTRA_SC_SAST_LOGIN_OPTS	No	Specify additional Fortify ScanCentral SAST login options. For more information, see the Fortify CLI Documentation Manual Pages.
SSC_APPVERSION	No	Specify the Fortify Software Security Center application version to use with this action
EXTRA_PACKAGE_OPTS	No	Specify additional Fortify ScanCentral SAST package command options
EXTRA_SC_SAST_SCAN_OPTS	No	Specify additional Fortify Static Code Analyzer options
DO_WAIT	No	Set to `true` to have the action poll Fortify ScanCentral SAST for SAST scan completion
DO_EXPORT	No	Set to `true` to export scan results to the GitHub Security view of the repository.
TOOL_DEFINITIONS	No	Specify tool definitions.

4. Commit the changes made to the workflow.

Best practices and tips

- To simplify onboarding across an organization, you can create reusable workflows that are accessible from other repositories or starter workflows that serve as templates. See the GitHub Actions documentation for more information on creating reusable workflows or starter workflows.
- Integrating multiple repositories with one workflow can simplify the process of managing and deploying code across multiple projects. You can set this up with required workflows in an organization ruleset, which triggers for every pull request and blocks the merge if the pipeline

fails. Required workflows should be stored in a separate repository. See the GitHub Actions documentation for more information on creating organization rulesets and making workflows required.

- You can create organization secrets to avoid managing credentials for every repository. Credentials need the appropriate scope and application access. PATs are also subject to expiration. See the GitHub Actions documentation for more information on creating organization secrets.

Note: External documentation links might not refer to your version of GitHub.

opentext™

Support and Documentation

Contacting Customer Support

Visit the Support website to:

- Manage licenses and entitlements
- Create and manage technical assistance requests
- Browse documentation and knowledge articles
- Download software
- Explore the Community

https://www.microfocus.com/support

For More Information

For more information about Fortify software products:

https://www.microfocus.com/cyberres/application-security

About the Documentation Set

The Fortify Software documentation set contains installation, user, and deployment guides for all Fortify Software products and components. In addition, you will find technical notes and release notes that describe new features, known issues, and last-minute updates. You can access the latest versions of these documents from the following Product Documentation website:

https://www.microfocus.com/support/documentation

To be notified of documentation updates between releases, subscribe to Fortify Product Announcements on the OpenText Fortify Community:

https://community.microfocus.com/cyberres/fortify/w/announcements

Fortify Product Feature Videos

You can find videos that highlight Fortify products and features on the Fortify Unplugged YouTube channel:

https://www.youtube.com/c/FortifyUnplugged