Fortify's latest and greatest

What's new in Fortify software 24.4.0

At Fortify by OpenText™, we believe great code is secure code and helping customers achieve it runs through everything we do. Fortify continues to cover the most critical use cases common to today's software landscape. From DevSecOps and Cloud transformation to securing the software supply chain, Fortify is proud to be recognized by Gartner as a market leader in application security testing for the 10th year in a row.

We are excited to announce the general availability of our Fortify 24.4.0 release! With enhanced offerings to increase speed, accuracy, scalability, and ease of use, this marks another important chapter in Fortify's elevation of code security. This release contains updates to OpenText™ Static Application Security Testing (Fortify Static Code Analyzer), OpenText™ Dynamic Application Security Testing (Fortify WebInspect), Fortify Software Security Center, and Fortify Software Composition Analysis.

This release of Fortify Software includes the following new functions and features:

Fortify Software Security Center

The following features have been added to Fortify Software Security Center.

Technology Preview: OpenText™ Intelligence (Magellan) BI and Reporting dashboards

This release includes a preview of upcoming support for the inclusion of OpenText Intelligence BI and Reporting dashboards in Fortify Software Security Center. The dashboards provide a comprehensive application security program overview, insights into important vulnerability metrics, and consistent dashboard views among the Fortify product suite. If you are interested in previewing the upcoming dashboard integration, contact Customer Support for the software and support required to run the technology preview.

Audit Issue History Tracking

- You can track changes in the attributes of an issue as you upload new scans for an audit. The issue history includes all attributes that Fortify Software Security Center extracts from uploaded scans that can be searched or filtered on the audit page.

ScanCentral SAST Controller role

- The ScanCentral SAST Controller role is a new pre-configured role. This role is intended for use only when configuring a Fortify ScanCentral SAST Controller. It allows users who are permitted to run scans to upload them, even if they do not have upload analysis result permissions.

Kubernetes support

- Support added for Kubernetes versions 1.30 and 1.
- Support added for Helm command-line tool versions 3.15 and 3.16.

Fortify ScanCentral SAST

The following features have been added to Fortify ScanCentral SAST.

Uploading analysis results to Fortify Software Security Center

- You can configure the ScanCentral SAST Controller with a ScanCentral SAST Controller service account created in Fortify Software Security Center. This allows you to upload the scan results to Fortify Software Security Center using the Controller service account. In this case, your Software Security Center user accounts do not require the upload analysis results permission.
- The start command -uptoken option is no longer required to upload scan results to Fortify Software Security Center if you specify the -sscurl and -ssctoken option pair.

ScanCentral client

- You can add JVM system and ScanCentral SAST properties (for clients and sensors) to the ScanCentral client commands by adding the -D option to the SCANCENTRAL_VM_OPTS environment variable. You can add JVM system properties to the environment variable for use by the PackageScanner tool.
- You can retrieve your package (job file) from the Controller using the retrieve command –job-file option.
- The client start command -sargs option accepts the Fortify Static Code Analyzer -bin option.
- The client start command -targs option accepts the Fortify Static Code Analyzer -gotags option.
- When packaging PHP projects that use Composer for dependency management, the ScanCentral client will automatically restore the dependencies prior to generating the package.
- Support packaging Maven projects that use the -Dmaven.repo.local or -Dsettings.localRepository properties to configure a non-default local repository location.

Updated build tool support

- Support for Gradle 8.7 - 8.10

ScanCentral SAST containers

- New ScanCentral SAST Windows Sensor container with Windows Server 2022 as a base image
- New database migration container to migrate the ScanCentral SAST Controller database when upgrading

OpenText Static Application Security Testing

The following features have been added to OpenText Static Application Security Testing

Platforms

- Linux on ARM support
- IBM AIX 7.3

Languages

- .NET (Core) 9.x
- ABAP 7.x
- Angular 17
- Apex 61
- C# 13
- Go 1.23
- Kotlin 2.0
- PL/SQL 10, 11, 12, 18, 19, 21, and 23
- TypeScript 5.3 and 5.4

Build tools

- Bazel 7.x
- Gradle 8.5
- MSBuild 17.11
- MSBuild and Bicep support on .NET 8

Platforms and architectures

- Added support for IBM AIX 7.3.

Features/Updates

- Updated the scan policies with the ability to exclude dataflow issues based on taint flags
- Added support for Go build tags with the -gotags command-line option
- Added support for Flask framework and Jinja2 templates

OpenText Static Application Security Testing tools

The following features have been added to Fortify Static Code Analyzer tools.

Secure code plugins

- Support for Eclipse 2024-06
- Support for IntelliJ IDEA 2024.2
- Support for Android Studio 2023.3 and 2024.1
- Support for Azure DevOps Server 2022

Fortify ScanCentral DAST

The following features have been added to ScanCentral DAST.

Scan details now has Created By

The scan details panel now displays the user that created/imported the scan.

New REST endpoint to view messages

SC DAST has added an endpoint to retrieve the polling messages that occur in the product. These are primarily the message that the global service is processing from the sensors.

Linux containers now on UBI9

The SC DAST containers on Linux is now on the RedHat UBI9 with .NET 8.

Contact 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.

Get more information about Fortify software products.

OpenText Dynamic Application Security Testing

The following features have been added to OpenText Dynamic Application Security Testing

WebInspect CLI & API

Support has been added for using an external SQL Server database when using either the WebInspect CLI or the WebInspect API.

Expanded URL field

URL field has been expanded for API scans using a postman collection. This allows the user to view the authentication endpoints and proceed with a dynamic token strategy.

HAR improvements

Updates to the HAR parser allows for a greater number of formats from different browsers.

New logging option

New environment variable for logging to stderr output.

Linux containers now on UBI9

The Dynamic Application Security Testing container on Linux is now on the RedHat UBI9 with .NET 8.