Fortify Latest and Greatest

What’s New in Fortify 22.1.0

June 2022
What’s New in Fortify 22.1.0

**General Availability—Fortify 22.1.0 Release**

At Fortify, our goal is to assist organizations in building software resilience for modern development from a partner they can trust. Fortify continues to cover a wide range of AppSec use cases common to today’s landscape. From DevSecOps, Cloud Transformation, Securing the Software Supply Chain, and Maturity at Scale, Fortify delivers a holistic, inclusive, and extensible platform that supports the breadth of your software portfolio.

We are excited to announce the general availability of our Fortify 22.1.0 release! With enhanced offerings to increase speed, accuracy, scalability, and ease of use, this marks another important chapter in Fortify’s elevation of application and code security. Some highlights of this release include:

- Fortify continues our accelerated language support and invest in the platforms most important to our customers such as Java 17, .NET 6, and new support for Terraform HCL
- Scanning with workflow macros ensure important content is covered in scan. Now WebInspect can use HAR Files for workflow scanning.
- Out of Band Testing: WebInspect has the ability to test for a new class of vulnerabilities called Out of Band or OAST vulnerabilities. Using the public Fortify OAST server WI can detect OAS vulns such as Log4Shell

This release contains updates to Fortify Static Code Analyzer, Fortify WebInspect, Fortify Software Security Center, and Fortify Software Composition Analysis. The complete list of new functions and features include:

![Diagram of programming languages](image)
The following features have been added to Fortify Software Security Center.

**Issue Correlation Details**
If you have correlated issues in an application version, you can use the heading for the correlated issues icon to sort listed issues based on whether or not they are correlated with other issues (see “Viewing Correlated Issues on the AUDIT Page” in the Fortify Software Security Center User Guide). You can also selectively list the issues with which a given issue is correlated (see “Auditing Correlated Issues” in the Fortify Software Security Center User Guide).

**Targeted Rulepack Downloads**
Previously, Fortify Software Security Center ignored the clientType parameter in Rulepack update requests. As a result, Rulepack clients received all Rulepacks available (both Fortify Static Code Analyzer and Fortify Security Assistant Rulepacks). Now, Fortify Software Security Center takes the clientType parameter into account for Rulepack update requests. For details, see “Updating Rulepacks from the Micro Focus Fortify Update Server” in the Fortify Software Security Center User Guide.

**Updated Processing Rule: Ignore SCA Scans Performed in Quick Scan Mode**
The processing rule for ignoring Fortify Static Code Analyzer scans performed in quick scan mode now also prevents the upload of Fortify Static Code Analyzer speed dial results performed with a setting of less than four. For details, see “Setting Analysis Results Processing Rules for Application Versions” in the Fortify Software Security Center User Guide.

**Report Maintenance: New “Days to Preserve” Option**
On the Scheduler page, the Days to preserve option was added in a new Reports maintenance section. This option enables you to specify the number of days Fortify Software Security Center retains generated reports. For more information, see “Configuring Job Scheduler Settings in the Fortify Software Security Center User Guide.”

**Pausing Job Execution**
You can now control job execution by pausing (and then resuming) it using the Pause job execution option located on the Maintenance page (ADMINISTRATION > Maintenance). After you pause job
execution, jobs (artifact processing, report generation, data export requests, and so on) that are currently running continue to completion. Any new jobs submitted are queued for processing once the Pause job execution check box is cleared and normal processing resumes.

For more detail, see “Pausing and Resuming Job Execution” in the Fortify Software Security Center User Guide.

Requiring Comments for Specific Custom Tag Values
Administrators can now require comments for custom tags. When the “Require Comments” setting is checked, any changes to the custom tag will cause an additional comment box to appear for the custom tag and the Save button will be disabled until a comment is entered. For details, see “Adding Custom Tags to the System” in the Fortify Software Security Center User Guide.

Expanded Issue Counts
Previously, you could display 20, 50, or 100 issues at a time on the AUDIT page. Now, you can display up to 150 or 200 issues per page.

Kubernetes Updates
- Added support for Kubernetes 1.22
- Added support for Helm 3.8

Fortify ScanCentral SAST
The following features have been added to Fortify ScanCentral SAST.

Kotlin for Android Support
You can now use the ScanCentral Client to package Kotlin for Android projects for remote translation using Gradle integration (-bt gradle).

New Command to Update ScanCentral Client
Using the new update command, you can update ScanCentral Client to the latest version on the ScanCentral Controller.

Get SSC Artifact Processing State Using Job Token
Using the status command, ScanCentral Client can retrieve the processing state of a job that uploaded the FPR to SSC.

Build Tool Updates
- Gradle 7.3
- MSBuild 14.0, 17.0, 17.1, and 17.2

Support for Multiple Client Versions on the Controller for Auto-Update
The Auto-Update feature now supports multiple versions of clients. Sensors and embedded clients will be updated by the versions available in the Controller, rather than the version of the Controller.

Fortify Static Code Analyzer (Fortify SAST)
The following features have been added to Fortify Static Code Analyzer.

Operating System Updates
Fortify added support for the following operating systems and versions:
- macOS 12
- Windows 11

Compiler Updates
Fortify added support for the following compiler versions:
- Clang 13.1.6
- OpenJDK javac 17
- Swift 5.6
- cl (MSVC) 2015 and 2022

Build Tool Updates
Fortify added support for the following build tool versions:
- Gradle 7.4.x
- MSBuild 14.0, 17.0, 17.1 and 17.2
- Xcodebuild 13.3 and 13.3.1

Language and Framework Updates
- C# 10
- .NET 6.0
- C/C++ 20
- HCL 2.0
- Java 17
- TypeScript 4.4 and 4.5

Note: Rules for Terraform and Google Cloud Platform will be part of the Fortify Software Security Content 2022 R2 release.
Fortify Latest and Greatest

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

Visual Studio 2022 Support

IntelliJ 2021.x Support
The Fortify Analysis Plugin for IntelliJ now supports IntelliJ 2021.x to 2021.3.

Import Standard Fortify Rulepacks from Filesystem
Use the Options menu in Fortify Audit Workbench, Fortify Eclipse Complete Plugin, and Fortify Extension for Visual Studio to import Fortify Rulepacks downloaded from the Customer Portal.

Compare LOC of Scanned Files Between Two FPRs
View LOC counts of analyzed files in an FPR (-loc) or compare LOC counts between two FPRs using FPRUtility (-loc, -compareTo).

Configurable Timeout for fortifyupdate
Configure the socket timeout for fortifyupdate using the rulepackupdate.SocketReadTimeoutSeconds property in the server.properties file. The default value is 180.

New Search Modifier: shortfilename
In Fortify Audit Workbench and the Fortify Plugins for Eclipse, you can use shortfilename as a search modifier in Issue Templates to filter or hide issues that match the file name. For full path matches, continue to use the file search modifier.

New OWASP Top 10 2021 Report
Generate new OWASP Top 10 Report (2021) from the following tools:
- Fortify Audit Workbench
- Fortify Extension for Visual Studio
- Fortify Remediation Plugin for Eclipse
- BIRTReportGenerator

Fortify ScanCentral DAST
The following features have been added to Fortify ScanCentral DAST.

User Configuration Restrictions
- New permissions allow you to bar scanning of specific domains or IP addresses.
- New Modify User permission required to allow user to modify a scan. A user who does not have this permission can only configure a scan URL, login macro, workflow macros, and network credentials. With this limited role, users can start scans, create scans from base settings, and view settings but not change them.

PostgresSQL Support
- Support for use of a PostgresSQL database.

Scan Import
- Import Scans into ScanCentral PostgresSQL database from Fortify WebInspect or Fortify WebInspect Enterprise.

Automated Deployment (Infrastructure as Code)
- Support for the fully automated deployment of ScanCentral DAST.

Rescan Button
- The Rescan button allows you to rescan and existing scan.

Fortify WebInspect (Fortify DAST)
The following features have been added to Fortify WebInspect.

Support for HAR Files
Scanning with workflow macros ensures that important content is covered in a scan. WebInspect can now use HAR files for workflow scanning.
Out-of-Band Testing
WebInspect can now test for a new class of vulnerabilities called Out-of-Band or OAST vulnerabilities. Using the public Fortify OAST server, WebInspect can detect OAST vulnerabilities such as Log4Shell.

Engine 7.0 Updates
Fortify continues to enhance its engines to improve scan coverage and performance. WebInspect 22.1.0 provides a faster crawl and audit, and better application support from the Web Macro Recorder with Macro Engine 7.0.

MS SQL AD Authentication Support
WebInspect 22.1.0 can now use a MS SQL Database using AD Authentication.

Windows 11 Support
WebInspect 22.1.0 is now supported on the Windows 11 operating system.

Azure SQL Database Support
WebInspect 22.1.0 can now use an Azure SQL Database for storing scan data.

Sensor Support for Fortify WebInspect Enterprise 21.2.0
WebInspect 22.1.0 can be configured as a sensor for Fortify WebInspect 21.2.0.

Contact Micro Focus Fortify Customer Support
If you have questions or comments about using this product, contact Micro Focus Fortify Customer Support using one of the following options.

To manage your support cases, acquire licenses, and manage your account: www.microfocus.com/support

For More Information
For more information about Fortify software products: www.microfocus.com/solutions/application-security