# Micro Focus Fortify Software, Version 21.2.0

## Release Notes

Document Release Date: November 2021, Latest Update 12/6/2021
Software Release Date: November 2021

# IN THIS RELEASE

This document provides installation and upgrade notes, known issues, and workarounds that apply to release 21.2.0 of the Fortify product suite.

This information is not available elsewhere in the product documentation. For information on new features in this release, see What's New in Micro Focus Fortify Software 21.2.0, which is downloadable from the Micro Focus Product Documentation website:

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

# FORTIFY DOCUMENTATION UPDATES

## Accessing Fortify Documentation

The Fortify Software documentation set contains installation, user, and deployment guides. 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 HTML or PDF versions of these documents from the Micro Focus Product Documentation website:

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

If you have trouble accessing our documentation, please contact Fortify Customer Support.

# INSTALLATION AND UPGRADE NOTES

Complete instructions for installing Fortify Software products are provided in the documentation for each product.

## Fortify ScanCentral SAST

The ScanCentral SAST client must be installed on a machine with a Java 11 runtime.

## Updating Security Content after a Fortify Software Security Center Upgrade

If you have upgraded your Fortify Software Security Center instance but you do not have the latest security content (Rulepacks and external metadata), some generated reports (related to 2011 CWE) might fail to produce accurate results. To solve this issue, update the security content. For instructions, see the *Micro Focus Fortify Software Security Center User Guide*.

# USAGE NOTES FOR THIS RELEASE

There is a landing page (https://fortify.github.io/) for our consolidated (Fortify on Demand + Fortify On-Premise) GitHub repository. It contains links to engineering documentation and the code to several projects, including a parser sample, our plugin framework, and our JavaScript Sandbox Project.

## Fortify Static Code Analyzer

- Structural results: Most structural issues will show new instance IDs. The algorithm that computes instance IDs for structural issues now produces more variance than previous IDs that often differed only in the final digit.
- Kotlin: If you have Java code in your project that references Kotlin source, Kotlin functions called in Java are only resolved if the parameters and return types are built-in types or types defined in the same file as the called function definition.
- Most of the JAR files that were in the `default_jars` directory have been removed. For the majority of Fortify users, this will not have any effect. In exceptional cases it might lead to resolution errors and deteriorated results. This could be the case for projects that:
    - Are written in a JVM language (Java, Kotlin, or Scala) that are being translated manually (as opposed to scanning through Maven or Gradle integration),
    - Have an explicitly provided classpath that does not contain all dependencies, and some of the missing dependencies were present in `default_jars` in version 21.1.0 and earlier.

    The solution for projects that fall into these specific circumstances is to ensure that all dependencies are explicitly present in the classpath provided to sourceanalyzer.

- Java/Lombok: If your Java project uses Lombok @Log4j annotations, these annotations are only processed correctly if you include the appropriate log4j library in the classpath provided to sourceanalyzer with the –cp command-line option at translation time. Note that this does not apply to @Log4j2 annotations that use the log4j2 library.

## Fortify Software Security Center

- Swagger specification in Fortify Software Security Center version 21.1.X included legacy versions of action endpoints not present in 20.2. It was corrected in this release.
- A new permission, Use data exports, was added. It explicitly controls operations with Data exports. To maintain backward compatibility, the new permission was added to any existing role that already enabled users to work with Data exports. It includes both built-in roles and custom roles.
- Size of JSON submitted to SSC REST API is limited to 10 MB, which may affect huge bulk requests. Fortify does not recommend using requests larger than 10 MB,

but the limit can be adjusted by setting `rest.request.maxJsonSize` property to size in bytes in the `app.properties` file.
- The Kerberos/Spnego configuration is now validated internally. If you experience issues with a previously working SSO configuration, see the logs for more details. For the expected configuration format, see the Fortify Software Security Center User Guide.
- To improve security, Fortify Software Security Center will no longer announce Basic HTTP authentication on REST API endpoints using the WWW-Authenticate header. REST API clients must add the Authorization header explicitly.
- A new sample command-line based Software Security Center client (ssc-client) using REST API is now included in Software Security Center distribution. The `ssc-client` sample serves as a starting point for using a REST API-based client as a replacement for the SOAP API-based `fortifyclient`. See the ssc-client `README.md` for more details.
- SSC autoconfiguration with autoconfig file has been improved and the autoconfig is applied when Software Security Center is restarted if any autoconfig value has changed. Also, the handling of system environment variables for Software Security Center configuration has been changed. See the Fortify Software Security Center User Guide for details.

### Fortify ScanCentral SAST

- Due to a limitation in the way the Fortify ScanCentral SAST client currently collects files for remote translation of ASP.NET code, Fortify recommends that you run local translations and remote scans via Fortify ScanCentral SAST for ASP.NET projects.

### Fortify WebInspect, Fortify WebInspect Enterprise, and Fortify ScanCentral DAST

**NOTE**: The release date for WebInspect Enterprise version 21.2.0 is scheduled for the latter half of December 2021.

- Do not install the Functional Application Security Testing (FAST) proxy on the same machine as Fortify WebInspect, a Fortify WebInspect installation running the sensor service in a DAST environment, or a Fortify WebInspect sensor being used with Fortify WebInspect Enterprise.

## KNOWN ISSUES

The following are known problems and limitations in Fortify Software 21.2.0. The problems are grouped according to the product area affected.

### Fortify Software Security Center

This release has the following issues:

- When sending issues to Audit Assistant for training, you might need to click the SEND FOR TRAINING button twice to update the status.
- When servlet session persistence is enabled in Tomcat, a class invalid for deserialization exception might be thrown during Tomcat startup. This is caused by significant changes in the classes where instances can be stored in HTTP sessions. You can ignore this exception.
- Enabling the "Enhanced Security" option for BIRT reports will break report generation if Fortify Software Security Center is installed on a Windows system.
- For successful integration with Fortify WebInspect Enterprise, Fortify Software Security Center must be deployed to `/ssc` context. In particular, the context must be changed for Fortify Software Security Center Kubernetes deployment, which uses root context by default.
- Date and time preferences chosen for Fortify Software Security Center are not reflected for ScanCentral DAST. The ScanCentral DAST page still displays the default format of MM/DD/YYYY.
- By default, Micro Focus Fortify Software Security Center blocks uploaded speed dial analysis results performed with a precision level less than four (full scan). However, you can configure your Fortify Software Security Center application version to process speed dial analysis results. To allow speed dial analysis results to be uploaded to Fortify Software Security Center, clear the ”Ignore SCA scans performed in Quick Scan” processing rule for your application version. Once you have made a choice between uploading a full scan or speed dial analysis results, Fortify recommends that future scan results for the application version be of the same type.

## Fortify ScanCentral SAST

- In the Fortify ScanCentral SAST CLI, the `-targs` and `-sargs` options do not handle paths with spaces correctly. For example, `-targs "-exclude C:\My Project\src\Project1.java"` or `-targs -exclude -targs "C:\My Project\src\Project1.java"`. If using the `-targs` or `-sargs` options, make sure that no paths include spaces.

## Fortify Static Code Analyzer

This release has the following issues:

- While scanning JSP projects, you might notice a considerable increase in vulnerability counts in JSP-related categories (e.g. cross-site scripting) compared to earlier versions of Fortify Static Code Analyzer. To remove these spurious findings, specify the `-legacy-jsp-dataflow` option on the Fortify Static Code Analyzer command line during the analysis phase.

- Fortify Static Code Analyzer 21.2.0 is not compatible with MSBuild 14. We advise staying on Fortify Static Code Analyzer version 20.2.x if you need integration with MSBuild 14. A workaround is available to integrate MSBuild 14 with SCA 21.2.0. For instructions, please contact Micro Focus Fortify Customer Support.

## Fortify Audit Workbench, Secure Code Plugins, and Tools

This release has the following issues:

- Security Assistant for Eclipse requires an Internet connection for the first use. If you do not have an Internet connection, you will get an Updating Security Content error unless you copied the rules manually.
- Scan Wizard does not properly handle paths with spaces when using additional translation options in remote translation.
- The IntelliJ Analysis Plugin shows the version as 0.0.0 in IntelliJ IDEA versions 2021.2 and later. As a workaround, copy `Fortify_IntelliJ_Analysis_Plugin_21.2.0.zip\FortifyAnalysis\META-INF\plugin.xml` to `Fortify_IntelliJ_Analysis_Plugin_21.2.0.zip\FortifyAnalysis\lib\com.hp.fortify.intellij.analysis-21.2.0.<build number>.jar\META-INF\plugin.xml` (overwrite the file). Then install the plugin.
- The IntelliJ Remediation Plugin does not work in IntelliJ IDEA/WebStorm/PyCharm versions 2021.2 and later (and is not officially supported). As a workaround, copy the `Fortify_IntelliJ_Remediation_Plugin_21.2.0.zip\Fortify\META-INF\plugin.xml` to `Fortify_IntelliJ_Remediation_Plugin_21.2.0.zip\Fortify\lib\com.fortify.dev.ide.intellij-21.2.0.<build number>.jar\META-INF\`. Then install the plugin.

## Fortify ScanCentral DAST

This release has the following issue:

- In Fortify Software Security Center, you can change the date format from MM/DD/YYYY to YYYY/MM/DD. Fortify ScanCentral DAST does not inherit this setting from Software Security Center. Keep this in mind if you change the date format.

# NOTICES OF PLANNED CHANGES

Note: For a list of technologies that will lose support in the next release, please see the "Technologies to Lose Support in the Next Release" topic in the Micro Focus Fortify Software System Requirements document. This section relates to features that will change or be removed in the near future.

## Fortify Software Security Center

- REST API token endpoint /api/v1/auth/token is disabled by default and scheduled for removal. Please use the /api/v1/tokens endpoint instead.

- Fortify recommends the use of REST API (/api/v1/* and /download/*) endpoints instead of SOAP API (/fm-ws/*) endpoints. While you can still use the SOAP API, we are in the process of deprecating SOAP API support.

- The Seven Pernicious Kingdoms report is no longer supported and will be removed in the next release.

### Fortify Static Code Analyzer

- Support for the GOPATH will be removed to align with changes in the Go language.

### Fortify Audit Workbench, Secure Code Plugins, and Tools

- Security Assistant for Eclipse will not be included in the Fortify_SCA_and_Apps_<version>_<OS>.zip in the next release. It will be available for download from the Eclipse Marketplace.
- The following tools will not be included with the Fortify Static Code Analyzer installer: Audit Workbench, Custom Rules Editor, Secure Code Plugins, Scan Wizard, fprutility, reportgenerator, birtreportgenerator, fortifyclient, packagescanner, and scancentral in the next release. These tools will require different installers.

### Fortify WebInspect

- Fortify WebInspect will remove support for Flash parsing in the next release.

## FEATURES NOT SUPPORTED IN THIS RELEASE

The following features will no longer be supported in the next release. Features that are identified as deprecated represent features that are no longer recommended for use. In most cases, the deprecated item will be removed from the product in a future release. Fortify recommends that you remove the deprecated feature from your workflow at your earliest convenience.

- Fortify Static Code Analyzer no longer supports Visual Studio Web Site projects. You must convert your Web Site projects to Web Application projects to ensure that Fortify Static Code Analyzer can scan them.
- The CloudCtrlToken token type has been removed. Use the ScanCentralCtrlToken instead.

**Note**: For a list of technologies that are no longer supported in this release, please see the "Technologies no Longer Supported in this Release" topic in the Micro Focus Fortify Software System Requirements document. This list only includes features that have lost support in this release.

## SUPPORT

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

To Manage Your Support Cases, Acquire Licenses, and Manage Your Account: https://www.microfocus.com/support.

# LEGAL NOTICES



## Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

## Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.