Micro Focus Fortify Software v21.1.0

Release Notes

Document Release Date: August 9, 2021
Software Release Date: July 13, 2021

IN THIS RELEASE

This document provides installation and upgrade notes, known issues, and workarounds that apply to release 21.1.0 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 21.1.0, 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.

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.
- COBOL: If you plan to scan COBOL on a Windows system via automation, update the group policy so that Error Reporting does not require user intervention when an error occurs.
    1. Click the Windows **Start** button.
    2. Type `gpedit.msc`
    3. Navigate to `Computer Configuration->Administrative Templates->Windows Components->Windows Error Reporting`
    4. In the right pane, click on `Prevent display of the user interface for critical errors` and set it to `Enabled`.
- 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.

Fortify Software Security Center

- REST API token endpoint `/api/v1/auth/obtain_token` was removed. Please use the `/api/v1/tokens` endpoint instead.
- Endpoint `/api/v1/auth/token` has been disabled by default. `/api/v1/tokens` should be used instead. If you use the Fortify Extension for Visual Studio or Fortify Audit Workbench version 20.2.x or earlier, connect to Fortify Software Security Center using the X.509 or Kerberos SSO authentication method and enable the `/api/v1/auth/token` endpoint using the following property `<fortify.home>/<app_context>/conf/app.properties` file: `rest.enableLegacyTokenEndpoint=true`. We recommend that you enable the legacy endpoint only for the transitional phase and remove the property after Fortify Extension for Visual Studio and Fortify Audit Workbench are upgraded to 21.1.x.

- The Governance module, which has been obsolete for some time, has been removed. We also removed several endpoints, tables, and alerts:
    - The following endpoints were removed: `/upload/documentArtifactUpload.html`, `/download/documentArtifactDownload.html`, `/download/activitySignOffFprDownload.html`, `/download/requirementTemplateSignOffFprDownload.html`.
    - The following SOAP endpoints perform no actions: *`uploadDocumentArtifact`*, *`downloadArtifact`*
    - SSC Report Templates for Application Summary, Security at a Glance, Hierarchical Summary and Issue Trending reports were updated and no longer query removed database tables. If you use custom generated Report Templates, especially if based on aforementioned templates, make sure your templates do not query any of the removed tables: *activitycomment*, *activityinstance*, *activitysignoff*, *documentai*, *documentartifact*, *documentartifact_def*, *documentdefinstance*, *measurementinstance*, *projectstateai*, *requirementcomment*, *requirementinstance*, *requirementsignoff*, *requirementtemplatecomment*, *requirementtemplateinstance*, *requirementtemplatesignoff*, *savedevidence*, *sdlhistory*, *taskcomment*, *taskinstance*, *timelapse_event*, *timelapseai*, *variableinstance*
    - If you have system alerts that monitor Governance events (`Document Artifact Created/Updated/Deleted, Due Date Updated, Persona Assignment Updated, Work Owner Updated`), extract any data you wish to preserve for future reference from these alerts (e.g. list of monitored application versions). These alerts will never trigger and will be removed by migration.
- The unused `userOnly` flag caused confusion so it has been removed from the payloads of the `/roles` and `/authEntities/{parentId}/roles` endpoints (where it was ignored) and `/permissions` and `/roles/{parentId}/permissions` endpoints (where its value was always false and had no real use). We recommend that you remove this flag from any scripts calling these endpoints.
- The `userType` (SSO/LOCAL) read-only flag was exposed in `/localUsers` endpoint payloads. For a long time, only LOCAL user types have been used in Fortify Software Security Center and represent users with standard functionality. SSO user types will not be able to log in to Fortify Software Security Center using username + password authentication anymore. Any legacy local users of SSO user type with existing password will be migrated to LOCAL user type to preserve their ability to log in.
- To improve security, the `ssc-webapp` container does not run with privileged user (UID 0) anymore. The container will run with a standard user (UID 1111). Migration is handled automatically by distributed SSC Helm chart.
- It is not necessary to provide `db.driver.class`, `db.dialect` and `db.like.specialCharacters properties` when automating Fortify Software Security Center configuration using

`autoconfig` file anymore. Although values for these properties are ignored if included in `autoconfig`, Fortify recommends removing them.

- The JDBC driver for Oracle database server is now distributed with Fortify Software Security Center.
- Access to the legacy SOAP `InvalidateTokenRequest` and `GetAuthenticationTokenRequest` have been removed from the default token types. Although these requests can still be granted in custom token definitions, access via token authentication will be explicitly denied in the future.
- When integrating Fortify WebInspect Enterprise / ScanCentral DAST / Audit Workbench or other Fortify Tools with Fortify Software Security Center, clock skew must be minimized between the different communicating machines (suggested: less than 5 minutes, compared on UTC basis). Requests to Fortify Software Security Center can fail if there is excessive clock skew.

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

- 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 21.1.0. 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 may 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 may 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.
- You cannot enable `Enhanced security, security manager` for BIRT reports if your Fortify Software Security Center is installed on a Windows system.

- An `Authentication object was not found in the SecurityContext` error might occur for requests to REST API with both session ID and token present. To avoid this, use either session or token in a single request, but never both. If a token is available, use token only.
- A Fortify Software Security Center docker container deployment cannot integrate with Fortify WebInspect Enterprise. Additionally, the standard Fortify Software Security Center must be deployed to /ssc.

Fortify ScanCentral SAST

- In the Fortify ScanCentral SAST CLI, use the '/switch' form instead of '-switch' for the '`-bc (--build-command)`' option when using 'msbuild' for the '`-bt (--build-tool)`' option.

Fortify Static Code Analyzer

This release has the following issues:

- Due to major improvements in our scanning capabilities for Go, PHP, Kotlin and Python, some issues will be assigned a new Instance ID and marked as New. The previous finding will be marked as removed.
- Visual Studio 2019 update 16.7 and later brings .NET Core SDK 3.1.403, which is not yet supported by Fortify Static Code Analyzer and can result in translation issues. As a workaround, Fortify recommends you downgrade the .NET Core SDK to version 3.1.109 (the latest version that Fortify Static Code Analyzer currently supports).
- Fortify Static Code Analyzer 21.1.0 is not compatible with MSBuild 14. We advise staying on Fortify Static Code Analyzer verion 20.2.x if you need integration with MSBuild 14. A workaround is available to integrate MSBuild 14 with SCA 21.1.0. For instructions, please contact support.
- MSBuild versions 16.10 and later are not yet supported by FortiFfy Static Code Analyzer. As Visual Studio 2019 comes with a corresponding version of MSBuild, we advise not upgrading Visual Studio 2019 to version 16.10 or later at this time to avoid running into this issue.

Fortify Audit Workbench, Secure Code Plugins, and Extensions

This release has the following issue:

- 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.

Fortify ScanCentral DAST

This release has the following issues:

- You may receive an `AUTH SETTINGS HAVE BEEN CHANGED AND MUST BE VALIDATED` message and a Validate button on your display after importing and validating a Postman collection file that uses Dynamic Authentication in the Scan Settings Configuration wizard. If this occurs and there are no errors or changes to the settings in the Postman Validation dialog box, click Validate.
  After the settings have been validated again, click OK to accept the settings.
- If you change any settings in the Postman Validation dialog box and validation of the new settings fails, the wizard displays a Validate button and the following message:
  `AUTH SETTINGS HAVE BEEN CHANGED AND MUST BE VALIDATED`
  After you correct the errors, click OK to update the values before you click the Validate button.
- ScanCentral DAST does not support Global variables or Data variables in Postman. However, it does support Environment and Collection variables as well as Local variables in a collection. Workaround: You can specify Global variables and Data variables in an Environment, which is a set of variables that you can use in your Postman requests.

Fortify WebInspect

This release has the following issue:

- WebInspect does not support Global variables or Data variables in Postman. However, it does support Environment and Collection variables as well as Local variables in a collection. Workaround: You can specify Global variables and Data variables in an Environment, which is a set of variables that you can use in your Postman requests.

Fortify WebInspect Tools

This release has the following issue:

- Conducting a scan with a macro that uses automatic logout detection and that was recorded in the Web Macro Recorder with Macro Engine 5.x may yield undesirable results. Fortify recommends that you remove the previously-detected logout condition as follows:

  1. Open the existing macro in the Web Macro Recorder with Macro Engine 6.0.
  2. Open the Logout Condition Editor.
  3. Delete the existing automatic logout condition.
  4. Play the macro. A new logout condition is automatically detected.

  For more information, including procedures for using the Logout Condition Editor, see the Web Macro Recorder with Macro Engine 6.0 help or the Micro Focus Fortify WebInspect Tools Guide.

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 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 removing SOAP API support.
- Use the new `ScanCentralCtrlToken` token type instead of `CloudCtrlToken`. The `CloudCtrlToken` token type will be removed in the next release.

Fortify ScanCentral SAST

- The Fortify ScanCentral SAST CLI `--exclude-disabled-projects (-edp)` option for the start and package commands will be removed in the next release.

Fortify Static Code Analyzer

- Visual Studio Web Site projects will not be supported in the next release. Please convert your Web Site projects to Web Application projects to ensure that Fortify Static Code Analyzer can scan them in the future.
- Support for the GOPATH will be removed to align with changes in the Go language.

FEATURES NOT SUPPORTED IN THIS RELEASE

- FindBugs integration in Fortify Static Code Analyzer is no longer supported.
- The following reports have been removed from Fortify Software Security Center: DISA STIG 3.x, SSA Application, and SSA Portfolio.
- DISA STIG 3.x mappings have been removed. This means the attributes associated with DISA STIG 3.x are no longer displayed in the Group By and Filter By lists on the Audit page in Fortify Software Security Center.

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.