Micro Focus Fortify Software, Version 22.2.0
Release Notes
Document Release Date: November 2022, updated: 1/31/2023
Software Release Date: November 2022

IN THIS RELEASE

This document provides installation and upgrade notes, known issues, and workarounds that apply to release 22.2.0 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 22.2.0*, which is available on 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 may find technical notes and release notes that describe forthcoming 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.

- The *Micro Focus Fortify Plugin for Eclipse User Guide* now covers only the Fortify Eclipse Complete Plugin. The new document *Micro Focus Fortify Remediation Plugin for Eclipse User Guide* describes the Fortify Remediation plugin for Eclipse.
- The *Micro Focus Fortify Plugins for JetBrains IDEs and Android Studio User Guide* has been renamed to *Micro Focus Fortify Analysis Plugin for IntelliJ IDEA and Android Studio User Guide* and covers only the Fortify Analysis plugin. A new document *Micro Focus Fortify Remediation Plugin for IntelliJ IDEA and Android Studio User Guide* describes the Fortify Remediation plugin.
- Support for versions of the GNU gcc and GNU g++ compilers has been expanded to 6.x – 10.4 on Windows, Linux, and macOS operating systems. This change is documented in the Compiler section of the *Micro Focus Fortify Software System Requirements*.

INSTALLATION AND UPGRADE NOTES

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

Fortify Static Code Analyzer

Migrating from a Patched Release of Fortify Static Code Analyzer: If your Fortify Static Code Analyzer installation has been patched, the last digit in the version number will be greater than zero. For instance, release 21.2.0 has a zero as the last digit which identifies it as a major release that has not been patched. Versions 20.1.6, 20.2.4, 21.1.4, and 21.2.3 are examples of patched releases. When upgrading from a patched Fortify Static Code Analyzer release, your configuration files and properties (`fortify-sca.properties`) might not carry over to the new installation. If you would like to migrate your configuration and properties settings to the new installation, please contact Fortify Customer Support for assistance.

Fortify Audit Workbench, Secure Code Plugins, and Tools

- Eclipse Remediation Plugin is not included in the `Fortify_SCA_and_Apps_<version>_<OS>.zip` in this release. It is available for download from the Eclipse Marketplace.
- IntelliJ IDEA and Android Studio Remediation Plugin is not included in the *Fortify_SCA_and_Apps_<version>_<OS>.zip* in this release. It is available for download from the JetBrains Marketplace.

USAGE NOTES FOR THIS RELEASE

There is a landing page (https://fortify.github.io/) for our consolidated (Fortify on Demand + Fortify On-Premises) 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

- The SCAState utility does not work in the 22.2.0 release. This functionality will be restored in the upcoming 22.2.1 patch. If you require the SCAState functionality in the 22.2.0 release, you can request a hotfix through Customer Support.
- For security reasons, Fortify Static Code Analyzer sample projects have been removed from the installer. These samples are now available as a separate ZIP package.

Fortify Software Security Center

- Recent Chrome or Chromium-based browsers default to `SameSite=Lax` cookie policy. That means cookies are not sent with sub-requests to 3rd-party sites. Therefore, SAML

Single Logout will not work correctly in cases when it is not initiated from Fortify Software Security Center. To make SAML Single Logout work in Chrome or Chromium-based browsers, SameSite policy for session cookies must be changed to “None”. Please note that this denotes less secure policy than the default one, so changing it is left for your consideration. To change the policy for container deployments, use `HTTP_SERVER_SAME_SITE_COOKIES` environment variable. For non-container deployments, add `<CookieProcessor sameSiteCookies="none"/>` to the context section of your Tomcat configuration. See https://tomcat.apache.org/tomcat-9.0-doc/config/context.html#Nested_Components for details. Fortify Software Security Center must be restarted for the changes to have effect.

- A major upgrade of libraries providing functionality for SAML Single Sign On and Single Logout solutions was delivered in this release. Fortify strongly recommends to test SAML SSO behavior after upgrade on non-production environment first. For successful SAML SSO migration, please follow the instructions below right after upgrading to 22.2.0.
    - HTTP Redirect and HTTP POST bindings are supported, however only one at a time for inbound SAML messages. The default binding is set to HTTP POST. In case your IdP only supports HTTP Redirect (GET) for sending Single Logout messages (this is the case of e.g. Microsoft Azure AD) you must switch to HTTP Redirect binding for inbound Single Logout messages. Add `sso.saml.logout.binding.consume=REDIRECT` property to `app.properties`. Fortify Software Security Center must be restarted for the changes to have effect.
    - Navigate to `<hostname>:<port>/<context>/saml/metadata/<SP_alias>` to re-generate Fortify Software Security Center SAML metadata and re-upload them to your IdP server. To make the transition as smooth as possible, an effort was made for SAML SSO to work correctly after upgrade even with SAML metadata generated pre-22.2.0 release. However, it is necessary to update the metadata file in IdP server at your earliest convenience.
    - Please also note that
        - HTTP Artifact binding is not supported anymore.
        - Logout responses and Logout requests sent by IdP are required to be signed, Fortify Software Security Center will refuse to process them otherwise.
- If `host.url` property includes default port (443 for https or 8080 for http), Fortify Software Security Center will strip it as a part of URL normalization. This behavior can be changed by adding property `host.url.normalization.forcePort=true` to `app.properties`. When this property is used, `host.url` will be normalized to always include a port, adding a default one if none is specified.
- Velocity template engine libraries affecting bugtracker filing templates were upgraded in this release from version 1.7 to version 2.3. For detailed list of changes in 2.3 since 1.7 see https://velocity.apache.org/engine/2.3/upgrading.html. Custom bugtracker filing templates, or custom changes to built-in bugtracker templates might be affected by the listed changes. If so, custom template content needs to be manually updated. If you wish to maximize backward compatibility instead, add property

`templates.velocity.enhancedBackwardCompatibility=true` to `app.properties`. Please note that this is a best effort for maintaining backward compatibility and some manual changes might still be necessary.

- In previous releases, a PUT request to `ap/v1/issueTemplates/{id}` returned 200 even in case a non-existing Issue Template ID was used. Such request will fail with 409 from now on.
- Azure DevOps bug filing template was updated and now escapes HTML characters for issue deeplinks and bug attributes. In case this template was customized (specifically, the Description field was altered) in previous releases, the template update might not be applied in full range, and manual changes might be necessary. For more details on how to apply HTML escaping, please refer to "Editing tips" available when editing bug filing template's fields in Administration page.

Fortify ScanCentral SAST

- Due to an issue where scans fail because of very long generated build IDs (multi-modal projects), ScanCentral SAST now uses a hash string for the build ID.

KNOWN ISSUES

The following are known problems and limitations in Fortify Software 22.2.0. The problems are grouped according to the product area affected.

Fortify Software Security Center

- Enabling the "Enhanced Security" option for BIRT reports breaks 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.
- The migration script downloaded from the maintenance page will be saved to file with PDF extension when using Firefox. The contents of the file are accurate, and it can be used for migration upon changing the file extension to `.sql`.
- Fortify Software Security Center does not verify optional signature on SAML identity provider metadata even if it is present. Recommended mitigation is using file:// or https:// URL to provide identity provider's SAML metadata to Fortify Software Security Center (avoid using http:// URL).
- When editing Issue Templates in UI, it is not possible to replace the template file. As a workaround, `/upload/projectTemplateUpload.html` API endpoint can be used to replace existing template file.
- Fortify Software Security Center API Swagger spec contains two definitions that differ only in case:
  - Custom Tag used for assigning custom tag values to issues in an application version

  - Custom tag used for managing custom tags

Please pay attention when using tools to auto-generate API clients from Swagger spec. This might cause conflicts due to case insensitive process, and the generated client might need manual modification.

Fortify Static Code Analyzer

- While scanning JSP projects, you might notice a considerable increase in vulnerability counts in JSP-related categories (e.g. cross-site scripting) compared to versions of Fortify Static Code Analyzer prior to 22.1.0. To remove these spurious findings, specify the `-legacy-jsp-dataflow` option on the Fortify Static Code Analyzer command line during the analysis phase.
- In some circumstances when upgrading Fortify Static Code Analyzer to a new version, the custom settings in the `fortify-sca.properties` configuration file might not get migrated. As a workaround, copy the custom settings from the `fortify-sca.properties` configuration file from the old installation location to the new one.

Fortify Audit Workbench, Secure Code Plugins, and Tools

- If you encounter crashes with Audit Workbench on an older version of Linux make sure you have the required version 3.22 (or later) of the GTK3 library.
- Selecting File Bug for the first time on Linux produces an error, but it disappears if you click on the button the second time.
- Authenticating with Azure DevOps from the Eclipse Complete plugin results in an error message on Linux.
- Clearing the date-typed custom tag's value is not working from the Fortify Remediation plugin for IntelliJ.
- BIRT reports do not support generating the XLS file format anymore.
- If you are not connected to the internet, you will get an Updating Security Content error when you first start Fortify Security Assistant for Eclipse. After importing the rules, you will no longer get this error upon startup.

Fortify ScanCentral DAST

- Users who do not have permissions to create settings, and who click **EDIT** from the Settings List, cannot save the edited settings as a new template. As a workaround, these users can use the Settings Configuration wizard by clicking **NEW SCAN** or **NEW SETTINGS**.
- The Data Retention setting is not displayed in Base Settings. If Data Retention was set in Base Settings that were configured in ScanCentral DAST 22.1.0, then those settings still apply, but are not displayed in the UI. Also, if Data Retention is enabled at the Application level, then the setting will be applied to the Base Settings. The Data Retention setting is displayed in the scan Settings. If you create new templates or run scans using these settings, then the Data Retention setting will be applied.

- Container names for the DAST Sensor and Utility Service must not exceed 50 characters in Docker run commands or Docker compose files.
- ScanCentral DAST uploads the scanner service logs to the database, but there is no UI option to download the logs. To get the logs, use the following API endpoint:

  ```
  GET /api/v2/scans/{scanId}/download-dast-service-logs
  ```

  A ZIP file that may contain multiple ZIP files is downloaded. This is because each time a scan is paused, interrupted, or completed, the logs are uploaded to the database. A scan may be resumed on a different scanner each time the scan is paused or interrupted, and the logs are saved each time.

- When importing an HTTP archive (.har) file to use as a workflow macro, the file size is limited to 4 MB. To increase the file size limit to 30MB, run the following SQL command:

  ```
  IF NOT EXISTS (SELECT Id
  FROM ConfigurationSetting WHERE SettingName =
  'UtilityWorkerServiceSettings.MaxReceiveMessageSize')

  INSERT
  INTO ConfigurationSetting (SettingName, SettingValue, IsEn
  crypted)

  VALUES
  ('UtilityWorkerServiceSettings.MaxReceiveMessageSize',
  '31457280', 0)

  GO
  ```

- Global Restrictions and Application Settings Domain Restrictions are applied only for Standard Scans or API scans that use a start URL.
- The Fortify ScanCentral DAST download package that you obtain from the Software and License Download site includes the `scancentral-dast-config-linux.tar` file for Alpine Linux distribution. The documentation does not describe how to use the Apline Linux version, but instead describes the preferred `scancentral-dast-config-ubi.tar` file for RedHat Linux distribution. To obtain the RedHat Linux version, contact Micro Focus Fortify Customer Support.

Fortify WebInspect Enterprise

- Completed scan request data presented in the WebInspect Enterprise WebConsole - Scan Requests UI may be overwritten when a new scan request is submitted for the same application version in Fortify Software Security Center. This issue will be resolved in a hotfix to 22.2.0.

- When exporting a scan in XML format to import as an artifact to Fortify Software Security Center, fewer findings may be present in the imported file than were in the original scan.

NOTICES OF PLANNED CHANGES

This section includes product features that will be removed from a future release of the software. In some cases, the feature will be removed in the very next release. Features that are identified as deprecated represent features that are no longer recommended for use. In most cases, deprecated features will be completely removed from the product in a future release. Fortify recommends that you remove deprecated features from your workflow at your earliest convenience.

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.

Fortify Static Code Analyzer

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

Fortify Software Security Center

- SOAP API is deprecated and is scheduled for removal, together with `fortifyclient` and the `wsclient` library. Please use REST API `(/api/v1/*, /download/* and /transfer/*)` endpoints instead of SOAP API `(/fm-ws/*)` endpoints.
- SOAP API is deprecated and is scheduled for complete removal as of the Fortify Software Security Center 24.1.0 release. The phased deprecation is scheduled as follows:
  - In SSC version 23.1.0, SOAP remains the default
  - In SSC version 23.2.0, SOAP is disabled by default, but is not removed
  - In SSC version 24.1.0, SOAP is removed entirely

  Please use REST API (`/api/v1/*, /download/* and /transfer/*`) endpoints instead of SOAP API (`/fm-ws/*`) endpoints. A new sample command-line based Fortify Software Security Center client (`ssc-client`) using REST API is included in the Fortify 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`.

  Note: It is always possible that, because of schedule delays, SOAP will be removed entirely in a release later than SSC 24.1.0.

- Starting with 23.1.0 release, it will not be possible to suppress Plugin Framework's validation of engineType using system environment variable

FORTIFY_PLUGINS_PARSER_VULN_ENGINETYPECHECK or JVM system property fortify.plugins.parser.vuln.engineTypeCheck. Any third-party parsers failing the validation will cease to work. EngineType of the submitted vulnerabilities must be coherent with engineType provided in the plugin metadata.

- REST API endpoint api/v1/projectVersions/{parentId}/dynamicScanRequests/action/cancel was deprecated and is scheduled for removal.

Fortify WebInspect

- The Web Service Test Designer tool will be removed in a future release.

FEATURES NOT SUPPORTED IN THIS RELEASE

The following features are no longer supported.

- Fortify Software Security Center REST API token endpoint /api/v1/auth/token has been removed. Please use the /api/v1/tokens endpoint instead.
- 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.
- Fortify WebInspect no longer supports Flash parsing
- Fortify ScanCentral SAST -
The allow_insecure_clients_with_empty_token property, used to configure the Controller, was removed from the config.properties file

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.