Micro Focus Fortify Software, Version 23.1.0
Release Notes
Document Release Date: May 18, 2023, last updated July 27, 2023
Software Release Date: May 18, 2023

IN THIS RELEASE

This document provides installation and upgrade notes, known issues, and workarounds that apply to release 23.1.0 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 23.1.0*, which is available on the Micro Focus Product Documentation website:

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

FORTIFY DOCUMENTATION UPDATES

- A new document *Micro Focus Fortify Static Code Analyzer Applications and Tools Guide* describes how to install the Fortify Static Code Analyzer applications and command-line tools. It also describes the tools included with the installation.
- Starting with this release, we no longer offer the Fortify WebInspect 15-Day Trial. The documentation and help still reference this offer, but it is no longer available.

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.

INSTALLATION AND UPGRADE NOTES

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

Fortify Static Code Analyzer, Fortify Audit Workbench, Secure Code Plugins, and Tools

Important: We now have two installers for Fortify Static Code Analyer. Use the `Fortify_SCA` installer to install Fortify Static Code Analyzer, a Fortify ScanCentral SAST client, and fortifyupdate. Use the `Fortify_Apps_and_Tools` installer to install applications and tools including Fortify Audit Workbench, Fortify Custom Rules Editor, Fortify Scan Wizard, Fortify Eclipse Plugin, IntelliJ Analysis Plugin, Visual Studio Extension, BIRTReportGenerator, ReportGenerator, and fortifyclient.

Fortify ScanCentral SAST

When configuring a sensor machine for remote translation of .NET projects, the sensor machine requires .NET Framework 4.7.2 or higher and .NET 6.0. Without .NET 6.0, the sensor may accept the .NET remote translation job but the translation will fail.

Fortify ScanCentral DAST

ScanCentral DAST Sensor Database Schema Upgrade Required: ScanCentral DAST 23.1.0 requires a schema upgrade to the sensor database. If you attempt to run a scan before upgrading your sensor database schema, you will receive an error indicating "Schema upgrade is required."

Contact Fortify Customer Support to obtain the script to upgrade your sensor database.

Fortify WebInspect

- Starting in this release, WebInspect uses an SQLite database for SecureBase. If you have created your own SecureBase for use in your environment, be aware that the file extension has changed from SDF (filename SecureBase.sdf) to DB (filename SecureBase.db).
- Starting with this release, we no longer offer the Fortify WebInspect 15-Day Trial. The Register 15-Day Trial option was removed from the License Wizard.

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

- To translate Python Django Framework code, you must include the `-Dcom.fortify.sca.PythonV2=false` option.
- When using Xcode 14.3.1, SCA will log a warning that swift version 5.8.1 is not supported. However, Fortify has tested swift version 5.8.1 and consider it a fully supported version. The warning message will be removed in the SCA 23.1.1 patch release.

Fortify Software Security Center

- A major upgrade of libraries providing functionality for SAML Single Sign On and Single Logout solutions was delivered in 22.2.0 release. If you are migrating from a version of Fortify Software Security Center earlier than 22.2.0, make sure to follow the SAML migration steps listed in the *Micro Focus Fortify Software Release Notes, Version 22.2.0*.
- Changes were made to several endpoints using a parent ID in order to make the behavior consistent for users with and without Universal access. A request to endpoints with non-existing parent ID will always fail with a meaningful error message. Previously, some endpoints returned empty resources if called by a user with Universal access.

Example (but not a complete list): `/issues/{parentId}/auditHistory`, `/issues/{parentId}/attachments`, `/artifacts/{parentId}`/scans. To revert to previous behavior, add `permission.universalAccess.allowInvalidParentId=true` to `app.properties`. Beginning with the 24.1.0 release, you will no longer be able to use the property to revert to previous behavior.

- In previous releases, a `DELETE` request to `api/v1/tokens` with query parameter `all=true` to revoke all authentication tokens for currently logged-in user failed with a 409 response code if there were no tokens left to revoke. This request now returns 200.
- If you used uppercase letters in the `host.url` property hostname with SAML SSO enabled, the Fortify Software Security Center initiated SSO login might not work after migration depending on which IdP service is used. We do not expect issues when using Microsoft Azure AD or AD FS. SSO logout and IdP initiated SSO login will not work (regardless of IdP service).

  To fully resolve these issues:

  - Regenerate the Fortify Software Security System SAML metadata after migration and update them in your IdP server. This is recommended if the breakage does not critically affect Fortify Software Security Center users.
  - For a smoother transition, add *host.url.normalization.lowerCaseHost=true* to `app.properties`. Fortify Software Security Center must be restarted for the change to take effect. This enables backward compatible SAML behavior. Generate Fortify Software Security Center SAML metadata and edit them manually: lowercase hostname part of Fortify Software Security Center URL in all Location and ResponseLocation attributes.

    Example: Change https://MyHost.test/SSC/saml/SingleLogout/alias/fortify_ssc to https://myhost.test/SSC/saml/SingleLogout/alias/fortify_ssc. Immediately after the modified metadata is uploaded to your IdP server, remove `host.url.normalization.lowerCaseHost=true` from `app.properties` and restart Fortify Software Security Center.

A letter-case normalization was introduced for the `host.url` property (Fortify Software Security Center URL). All letters in the host will be lowercased by default. SAML integration was affected by this change.

- Beginning with this release, Fortify Software Security Center now supports both REDIRECT and POST SAML logout bindings at once. It is no longer necessary to switch between them using the `sso.saml.logout.binding.consume` property. The property value is now ignored and Fortify recommends removing it from your Fortify Software Security Center configuration. This change does not affect existing SAML integrations but Fortify recommends that you regenerate Fortify Software Security Center SAML metadata an upload them to your IdP to keep the configurations synchronized.

- A typo was corrected in Helm chart values: `jmvTruststorePasswordEntry` was changed to `jvmTruststorePasswordEntry`. The change is backward compatible – if the property with the typo is used in your Helm chart, the Helm chart renders as expected. If both values are specified, the correct spelling takes precedence over the one with the typo. Fortify recommends you update your Helm chart value with the corrected property name.
- In earlier releases, the REST API purge by date action (`api/v1/projectVersions/action/purge`) failed with a 500 response code if no artifacts were eligible for purging. This request now returns 200.
- Local (Fortify) users logged in via the SSO method will not have the option to change their local password via User menu. To allow this, add `sso.local.password.change.allowed=false` to `app.properties` and restart Fortify Software Security Center. **Note**: the local password is not used in the SSO authentication flow.
- The MSSQL JDBC driver distributed with Fortify Software Security Center requires an encrypted connection by default and a trusted server certificate. Please refer to corresponding JDBC release notes https://learn.microsoft.com/en-us/sql/connect/jdbc/release-notes-for-the-jdbc-driver?view=sql-server-ver16 (MSSQL JDBC driver was upgraded to version 11.2.1.jre11, for changes in encryption, please refer to the “Changes in 10.2” section) and the documentation https://learn.microsoft.com/en-us/sql/connect/jdbc/connecting-with-ssl-encryption?view=sql-server-ver15 for more details.
- Please note following important changes related to SOAP API scheduled removal:
  - Logging any usage of SOAP API can be activated by setting a java system property `ssc.log.soap.level=info`. SOAP API requests will be logged to a separate `ssc_soap.log`. The log file is created on demand. This property is an easy way to identify if there are any SOAP API requests made to your Fortify Software Security Center instance.
  - A `soap.api.disabled` property is now available in `app.properties`. The default value is false. If switched to true, all SOAP API requests will be rejected with a "410 Gone" response.
  - The SOAP API based fortifyclient is the primary fortifyclient utility. It is in the `Tools/fortifyclient` folder.
  - The SOAP API based fortifyclient sample was removed from Samples folder.
  - The wsclient sample was removed and is no longer distributed under Samples folder.
  - A REST API based fortifyclient is now available. It is located in an alternate folder: `Tools/fortifyclient-new-rest/` folder.
  - REST API based fortifyclient is also available as a sample in the Samples folder.
  - About REST API based fortifyclient:

    Both the SOAP and REST versions of fortifyclient are called fortifyclient to aid in the transition. However, Fortify recommends the use of the new REST API based fortifyclient tool in your environment to ensure parity has been achieved between the SOAP and REST versions. Please report any missing or insufficient functionality to Fortify Customer Support so it can be addressed prior to the complete removal of SOAP API in 24.1.0.

Please note the following behaviors of the REST fortifyclient are different from that of the SOAP fortifyclient:

- When listing tokens using the REST fortifyclient listtokens command, session tokens (tokens associated to a session created automatically by Fortify Software Security Center) are not listed and the creation IP address is not included in the output listing.
- The REST fortifyclient accepts username + password authentication only for listtokens, invalidatetoken, and token commands. For any other command, token authentication must be used.

KNOWN ISSUES

The following are known problems and limitations in Fortify Software 23.1.0. The problems are grouped according to the product area affected.

Fortify Software Security Center

- MS SQL database may fail when FPR uploads occur out of sequence.
- 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 a `/ssc` context. The context must be changed for a 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 a 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`).
- Fortify Software Security Center API Swagger spec contains two definitions that differ only in case:
  - `Custom Tag` is used for assigning custom tag values to issues in an application version.
  - `Custom tag` is used for managing custom tags.

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

- If you enable DAST integration on the Administration page and navigate to **ScanCentral -> DAST** tab right away, the DAST page will not load. Reload the browser page to resolve this issue. This problem only occurs after enabling DAST.
- When uploading a custom rulepack the file encoding must be supported by the system's character set or the Tomcat java option "`-Dfile.encoding`" must be set to a compatible character set. If a non-compatible character set is used there will be an internal parsing error.

Fortify Static Code Analyzer

- When using Fortify Security Content 2023 Update 1 and Fortify Static Code Analyzer 23.1.0 or later, Fortify provides a default set of strict regular expression rules that can be customized using properties defined in the `<sca_install_dir>/Core/config/fortify-rules.properties` file. The new default rules are stricter than in previous releases in order to minimize false positives.

Fortify Audit Workbench, Secure Code Plugins, and Tools

- The IntelliJ Analysis plugin Test Connection on the ScanCentral SAST Configuration page might fail, however the actual ScanCentral upload should work as expected.
- 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.

Fortify ScanCentral DAST, OAST, WebInspect, and 2FA Server UBI Base Docker Image Names

Due to frequent base image updates caused by UBI security fixes, Fortify no longer includes the minor version for UBI base images for the ScanCentral DAST, OAST, WebInspect, and 2FA Server products or product components.

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 Software Security Center

The SOAP API has been deprecated and is scheduled for removal.

Important changes in Fortify Software Security Center version 23.1.0

- Please use REST API (`/api/v1/*, /download/* and /transfer/`*) endpoints instead of SOAP API (`/fm-ws/*`) endpoints.
- Logging usage of the SOAP API can be activated by setting a java system property `ssc.log.soap.level=info`. SOAP API requests will be logged to a separate `ssc_soap.log`. The log file is created on demand. This property is an easy way to identify if there are any SOAP API requests made to your Fortify Software Security Center instance.

- A `soap.api.disabled` property is now available in `app.properties`. The default value is false. If set to true, all SOAP API requests will be rejected with a "410 Gone" response.
- The SOAP API based fortifyclient is the primary fortifyclient utility. It is located in the `Tools/fortifyclient` folder.
- The REST API based fortifyclient is now available. It is located in an alternate folder: `Tools/fortifyclient-new-rest/` folder.
- The REST API based fortifyclient is also available as a sample in the Samples folder
- SOAP API based fortifyclient sample was removed from the Samples folder
- wsclient sample was removed and is no longer distributed in the Samples folder

SOAP API deprecation schedule:

Fortify Software Security Center version 23.1.0

- SOAP API is enabled by default
- Logging of any usage of SOAP API can be activated by the customer
- SOAP API can be disabled by the customer

Fortify Software Security Center version 23.2.0

- SOAP API is disabled by default
- Integration with Fortify Tools before version 23.2.0 is not supported unless SOAP API is explicitly enabled

Fortify Software Security Center version 24.1.0

- SOAP API is removed and cannot be enabled
- Integration with Fortify Tools before version 23.2.0 is not supported

About the REST API based fortifyclient:

Both the SOAP and REST versions of fortifyclient are called fortifyclient to aid in the transition. However, Fortify recommends the use of the new REST API based fortifyclient tool in your environment to ensure parity has been achieved between the SOAP and REST versions. Please report any missing or insufficient functionality to Fortify Customer Support so it can be addressed prior to the complete removal of the SOAP API in 24.1.0.

Please note that the following behaviors of the REST fortifyclient are different from those of the SOAP fortifyclient:

- When listing tokens using the REST fortifyclient listtokens command, session tokens (tokens associated to a session created automatically by Fortify Software Security Center) are not listed and the creation IP address is not included in the output listing.
- The REST fortifyclient accepts username + password authentication only for listtokens, invalidatetoken, and token commands. For any other command, token authentication must be used.

The SOAP API based fortifyclient deprecation schedule:

Fortify Software Security Center version 23.1.0

- SOAP API based fortifyclient is the primary fortifyclient utility. It is located in the `Tools/fortifyclient` folder.
- REST API based fortifyclient is now available. It is located in the `Tools/fortifyclient-new-rest/` folder.

Fortify Software Security Center version 23.2.0

- The REST API based fortifyclient will be the primary fortifyclient utility. It will be located in the `Tools/fortifyclient` folder.
- SOAP API based fortifyclient will continue to be available. It will be located in an alternate folder: `Tools/fortifyclient-legacy-soap/`
- Last opportunity to report any missing or insufficient functionality in the REST version of fortifyclient prior to deprecation of SOAP version in 24.1.0

Fortify Software Security Center version 24.1.0

- REST API based fortifyclient will be the primary fortifyclient. It will be in the `Tools/fortifyclient` folder.
- SOAP API based fortifyclient will be fully deprecated and no longer available

REST API endpoint `api/v1/projectVersions/{parentId}/dynamicScanRequests/action/cancel` was deprecated and will be removed in the next release.

REST API endpoint `/api/v1/projectVersions/{parentId}/issues/openSource` is deprecated and is scheduled for removal in 24.1.0 release. Please migrate to `/api/v1/projectVersions/{parentId}/dependencyScanIssues`.

The following reports and their mappings will be removed in the next SSR release and will be removed by default in Fortify Software Security Center 23.2.0:

- DISA STIG versions 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10
- SANS Top 25 versions 2009, 2010
- OWASP Top 10 versions 2004, 2007, 2010
- CWE Top 25 versions 2019, 2020
- WASC version 24 + 2

The removal of these mappings means the associated attributes associated will no longer be displayed in the Group By and Filter By lists on the Audit page of Fortify Software Security Center 23.2.0 nor any version of Fortify Software Security Center seeded with a bundle containing these changes.

Fortify WebInspect

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

Fortify WebInspect Enterprise

The next version of WebInspect Enterprise, version 23.2.0, will be the last version. Fortify recommends customers move to Fortify ScanCentral DAST for their dynamic scans.

Fortify ScanCentral SAST

- The `arguments` command is deprecated. Use the `start` or `package` command with either the `-targs` or `-sargs` option.

FEATURES NOT SUPPORTED IN THIS RELEASE

The following features are no longer supported.

- As previously announced, Fortify Software Security Center Plugin Framework's validation of `engineType` cannot be suppressed using system environment variable `FORTIFY_PLUGINS_PARSER_VULN_ENGINETYPECHECK` or JVM system property `fortify.plugins.parser.vuln.engineTypeCheck` anymore. 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.
- 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.

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