OpenText™ Fortify Software, Version 24.4.0
Release Notes

Document Release Date: October 2024
Software Release Date: October 2024

This document provides installation and upgrade notes, known issues, and workarounds that apply to release 24.4.0 of Fortify Software.

This information is not available elsewhere in the product documentation. For information on new features in this release, see *What's New in Fortify Software 24.4.0*, which is available on the Product Documentation website:

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

UPDATES TO THIS DOCUMENT

Date	Addition and/or change
10/31/2024	Initial release.

FORTIFY DOCUMENTATION UPDATES

The following languages are now supported in Fortify Software Security Center: Apex 61 and PL/SQL 23. The *System Requirements for Fortify Software* document will be updated to reflect this.

The link to Fortify Audit Assistant on Premises documentation has been changed. The new URL is: https://www.microfocus.com/documentation/fortify-audit-assistant/.

The *Fortify WebInspect Agent Installation Guide* and the *Fortify WebInspect Agent Rulepack Kit Guide* are no longer published. The information from these reference guides is now in the *Fortify WebInspect Agent Installation and Rulepack Kit Guide*.

Accessing Fortify Documentation

The Fortify Software documentation set contains installation, deployment, and user guides. In addition, you will find release notes that describe and last-

minute updates. You can access the latest HTML or PDF versions of these documents from the Product Documentation website:

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

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

INSTALLATION AND UPGRADE NOTES

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

Fortify License and Infrastructure Manager (LIM)

- The LIM now includes Secure Hash Algorithm (SHA) 256. Offline customers upgrading to 24.4.0 must perform an offline activation of the LIM from the Admin page to enable SHA256.

Fortify ScanCentral SAST

- If upgrading from version 23.1.x, use the DB migration script to migrate the Controller's database. If upgrading from a version prior to 23.1.x, first upgrade to 24.2.0 (using the migration script and starting the Controller once), then upgrade to 24.4.0 (no need to run the migration script).

Fortify Software Security Center

- This release includes a Technology Preview of OpenText™ Magellan™ BI & Reporting in Fortify Software Security Center. The preview provides a look at upcoming support for Magellan Dashboards. Starting with the next release, Magellan will be included in the Fortify Software Security Center deployment. To run the Technology Preview, you will need to install version 24.2 of OpenText™ Magellan™ BI & Reporting. Contact Customer Support to acquire the Magellan software and installation documentation.

- Helm chart and values file for Fortify Software Security Center deployment to a Kubernetes Cluster are no longer located in the Fortify Software Security Center distribution ZIP file. Steps for Kubernetes deployment have changed as well. For more details, refer to "Deploying Fortify Software Security Center to a Kubernetes Cluster" in the *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-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 License and Infrastructure Manager (LIM)

- Version 24.4.0 of the LIM and other Fortify products include both Secure Hash Algorithms (SHA) 1 and 256, which are used to verify communications between the LIM and other Fortify products. LIM version 24.4.0 can communicate with older versions of Fortify products that use only SHA1.

Fortify Static Code Analyzer

- For JavaScript/TypeScript projects, Fortify Static Code Analyzer 24.4.0 no longer reports findings in `node_modules` by default. To re-enable issue reporting in `node_modules` and restore 24.2.x release behavior, the property `com.fortify.sca.exclude.node.modules` should be set to false and specified at translation time.
- Updated LOC (lines of code) calculation: To better align with the LOC count shown by code editors, Fortify Static Code Analyzer now reports the total number of lines of code, including blank lines and comments. Due to this change, when you upload an artifact created with Fortify Static Code Analyzer 24.2.0 (or later) to an SSC application version that already contains artifacts generated by earlier versions of *Fortify Static Code Analyzer*, a one-time approval may be required if the following processing rule is enabled: `Require approval if line count differs by more than 10%`. After a 24.2.0 artifact has been

approved in an application version, subsequent 24.2.0 uploads to that application version will no longer trigger the processing rule unless the LOC count changes due to significant code changes or changes in the scan setup.

Fortify Software Security Center

- Significant improvements were delivered in Fortify Audit Assistant in the 23.2.0 release. If you are migrating from a version of Fortify Software Security Center earlier than 23.2.0, manual migration steps are required to continue using Fortify Audit Assistant integration. For more details, see "Updating the Fortify Audit Assistant Configuration" in the *Fortify Software Security Center User Guide* after upgrading.
- It is not possible to update `fileDocId` and `guid` field using PUT operation on `/api/v1/reportLibraries/{id}` endpoint anymore. These fields were never intended to be allowed to override.
- It is not possible to update `templateDocId` and `guid` field using PUT operation on `/api/v1/reportDefinition/{id}` endpoint anymore. Use POST operation on `/api/v1/reportDefinitions/{id}` to replace report template file. `Guid` field was never intended to be allowed to override.
- Obsolete and unused tables `runtimeapplication` and `applicationassignmentrule` are removed completely by migration. If you use custom Report Templates, make sure your templates do not query these tables.
- Starting from this release, if bulk request is authenticated with token or basic authentication, success login event is logged only for the bulk request itself, but not for all its sub-requests.
- A new query parameter `withoutCount` was added to listing REST API endpoints that use pagination, with default value false. The parameter can be used to disable computing the total object count for the 'count' response field. The parameter was added to improve performance specifically for `/api/v1/activityFeedEvents` endpoint. Setting the parameter to true might improve performance for some of the other

endpoints where it was added to, but the performance improvement is not expected universally. The addition of a new query parameter might require changes to code using swagger/openapi codegen to create API SDK. This applies at least to API SDK generated for Java.

- To differentiate token authentication from username/password authentication, Fortify Software Security Center is now using separate events for token authentication on REST API endpoints:

WS_LOGIN_SUCCESS (Web Services Authentication Succeeded)

WS_LOGIN_FAILURE (Web Services Authentication Failed)

WS_LOGIN_WITH_NO_ROLE (Web Services authenticated user has no permission)

KNOWN ISSUES

The following are known problems and limitations in Fortify Software 24.4.0. The problems are grouped according to the product area affected.

Fortify Software Security Center

- 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 to use file:// or https:// URL to provide the 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 the Swagger spec. It may cause conflicts due to its case insensitive process. The generated client might need manual modification.

- In some cases, users can experience the following error when creating application versions: “Access Denied. User <username> is not authorized. This permission is required to complete this action: [Manage application version access], or user does not have access to specified entity.” The application version is created, however, users selected to grant access in the last step of wizard will not be assigned to the application version. To work around this issue, do the following: 1. If the user has permission to "Add application versions to existing applications only" or "Add applications and application versions", add also "Manage application version access" permission. 2. If the user does not have "Add application versions to existing applications only" or "Add applications and application versions" permission, make sure that all the groups he is a member of, including nested membership, that have either "Add application versions to existing applications only" or "Add applications and application versions" permission, have also "Manage application version access" permission.

Fortify Applications and Tools

- In the Visual Studio Extension, if the Software Security Center URL is not specified, and you attempt to upload an FPR or open a collaborative audit, Visual Studio might crash. Make sure to configure the Software Security Center URL prior to performing these actions.
- In Audit Workbench, if you connect to a Jira Software Server with the bugtracker plugin and file a bug, then try to connect to Azure (TFS)

bugtracker, it will fail (and vice versa). If you need to connect to both Jira and Azure, you must connect to them in separate sessions.

- In Audit Workbench, Smart View does not work on Windows 11 and Windows Server 2022 because the default browser on these platforms is set to Edge. Changing the default browser to Chrome resolves this issue.
- Selecting File Bug for the first time on Linux produces an error, but it disappears if you click on the button a second time.

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. OpenText 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, see the "Technologies to Lose Support in the Next Release" topic in the *Fortify Software System Requirements* document.

Fortify Product Portfolio

Beginning in 2024, Fortify product GA versions will transition to be in parity with OpenText release versioning. Product versions will be based on the

targeted release year and quarter. This change only impacts product versions that do not currently follow this versioning strategy.

For example:

2023 release versioning

- Fortify Static Code Analyzer 23.1.0 *(release targeted for 2nd quarter 2023)*
- Fortify Static Code Analyzer 23.2.0 *(release targeted for 4th quarter 2023)*

2024 release versioning, and beyond

- Fortify Static Code Analyzer 24.2.0 *(release targeted for 2nd quarter 2024)*
- Fortify Static Code Analyzer 24.4.0 *(release targeted for 4th quarter 2024)*

Fortify License and Infrastructure Manager (LIM)

- Starting in version 25.4.0, the LIM and other Fortify products will include only Secure Hash Algorithm (SHA) 256. After that time, if you continue using a Fortify product earlier than 25.4.0, then you must also use a compatible version of the LIM.

Fortify ScanCentral SAST

- In version 25.2.0, the `replace_duplicate_scans` property in the Controller's `config.properties` file will default to "true". This means only one scan request per application version can be in the queue at a time (unless the scan request is sent with the `-dr` flag). Subsequent scan requests will replace the one in the queue.
- In version 25.2.0, the deprecated ARGUMENTS command will be removed from the ScanCentral SAST client.

Fortify Software Security Center

- Starting in 25.4.0 WIE (WebInspect Enterprise) support will be deprecated. In 26.4.0, WIE features will be removed from Fortify Software Security Center.
- Conservative, Aggressive and Exclusive job execution strategies are deprecated and will be removed in the next release. Automatic migration is not available. We recommend switching to Flexible job strategy. Instructions for replicating behaviors of the deprecated strategies can be found in the Fortify Software Security Center User Guide, chapter *"Configuring Job Scheduler Settings"*.
- Kerberos/SPNEGO and CAS single sign-on solutions are deprecated and will be removed from Fortify Software Security Center in the next release.
- Java Security Manger is deprecated in JDK 17 and subject for removal with no planned replacement in future JDK releases. Therefore, enabling Java Security Manager for BIRT reporting in Fortify Software Security Center ("Enhanced Security" option) is deprecated and will be removed in the next release.
- Note: For Fortify Software Security Center installed on a Windows system, "Enhanced Security" has been nonfunctional since version 20.2.0 due to usage of invalid paths containing a "<" symbol by BIRT runner. This made allowing access permission, which is necessary when Java Security Manager is enabled, impossible.
- Runtime-bridge utility JAR is deprecated and will be removed from Fortify Software Security Center in the next release.

Fortify Static Code Analyzer

- The modular analysis feature is deprecated and will be removed from the product in version 25.2.0.

Fortify ScanCentral DAST

- The DAST API v1 has been deprecated as indicated in the DAST API Swagger UI. It will be removed from the product in the 25.2.0 release.

- ScanCentral DAST 25.2.0 will include a new composite settings ZIP file that will replace the XML settings file format. ScanCentral DAST 25.2.0 will not support downloading the settings file in the XML format. Settings files downloaded from the ScanCentral DAST UI will be in the new composite settings ZIP file format. The following API endpoint will be disabled:

  /api/v<version:apiVersion>/application-version-scan-settings/<scanSettingsId:int>/download-scan-settings-xml

- Beginning with version 25.2.0, the ScanCentral DAST Configuration Tool CLI will not generate scripts or compose files. Sample files with descriptions will be provided instead.
- Version 25.4.0 will be the last release that includes Windows Docker images for ScanCentral DAST components. Afterwards, only Linux versions of Docker images will be available.

Fortify WebInspect

- Version 25.4.0 will be the last release that includes Windows Docker images for WebInspect. Afterwards, only Linux versions of Docker images will be available.
- Removal of the SOAP messaging protocol from Fortify WebInspect has been postponed until version 25.2.0. After upgrading to Fortify WebInspect version 25.2.0, you must also use a LIM version 22.1.0 or later that supports using the LIM REST API.
- The Web Service Test Designer tool will be removed in a future release.
- Guided Scan functionality will be removed in a future release.

Fortify WebInspect Enterprise

- Fortify WebInspect Enterprise has been discontinued. Version 23.2.0 was the last version of the product to be released. OpenText recommends that you move to Fortify ScanCentral DAST for your dynamic scans.

Fortify WebInspect SDK

- The Fortify WebInspect Software Development Kit (SDK) extension for Visual Studio will be deprecated in a future release.

Fortify Applications and Tools

- The Custom Rules Editor might be redesigned and replaced with an alternate tool in a future release of Fortify Static Code Analyzer Applications and Tools.

FEATURES NOT SUPPORTED IN THIS RELEASE

The following features are no longer supported.

Fortify Software Security Center

- Due to critical vulnerabilities in an open-source library unpatched in the upstream version with no plans to patch used by the Bugzilla plugin, this plugin is no longer being distributed with Fortify Software Security Center. OpenText recommends no longer using the Bugzilla plugin as the community libraries are not being actively supported and vulnerabilities in the libraries are not being effectively addressed. If you choose to accept the risk and continue to use Bugzilla plugin, you can keep using the plugin version you have already installed in Fortify Software Security Center after the migration. If you choose to continue using Bugzilla, in order to mitigate the issue, you must ensure that Fortify Software Security Center only connects to trusted Bugzilla servers over a secure connection. It includes requiring HTTPS for communication with the Bugzilla servers and allowing only trusted users to configure the Bugzilla plugin integration in Fortify Software Security Center.
- REST API POST operation at `/api/v1/issues/{parentId}/comments`, which was deprecated in 24.2.0, was removed in this release. Migrate to

`/api/v1/projectVersions/{parentId}/issues/action/audit`.

- REST API endpoints `/api/v1/personas` (Persona management) and `/api/v1/projectVersions/{parentId}/responsibilities` (lists and assigns responsibilities through Personas to a user for a given Application Version), which were deprecated in 24.2.0, were removed in this release with no replacement. The persona-based functionality is no longer used in Fortify Software Security Center.
- VSTSExtensionToken, which was deprecated in 24.2.0, was removed in this release. Already existing generated tokens of this type are revoked and removed during database migration. Use ScanCentralCtrlToken instead.

Fortify Static Code Analyzer

- The `-apex` and `-apex-version` options are deprecated and will be removed in a future release.
- 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 Applications and Tools

- Beginning with the 24.4.0 release, the Fortify Security Assistant Plugin for Eclipse will only be available from the Eclipse marketplace.

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

DEFINITIONS

DEPRECATION

When a product feature or integration is deprecated, OpenText no longer accepts enhancement requests for the feature but does respond to critical or

security defects. OpenText will continue to support the usage of a deprecated feature or integration. If applicable, the feature is turned off by default, but customers can re-enable it. OpenText will stop supporting the feature or integration on the removal date or in the removal release.

REMOVAL

When a product feature or integration is removed, OpenText no longer accepts or responds to critical or security defects. If the feature is a function, coded in the product, all code is removed, and the feature no longer functions in the product. If the feature is an external system or integration, the ability to integrate or be used by the product is removed and OpenText no longer supports its use or ability to function.

SUPPORT

If you have questions or comments about using this product, contact 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.