OpenText™ Application Security (Fortify) Software, Version 25.2.0
Release Notes

Document Release Date: May 2025
Software Release Date: May 2025

This document provides installation and upgrade notes, known issues, and workarounds that apply to release 25.2.0 of Application Security (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 Application Security (Fortify) Software 25.2.0*, which is available on the Product Documentation website:

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

UPDATES TO THIS DOCUMENT

Date	Addition and/or change
5/22/2024	Initial release.

FORTIFY DOCUMENTATION UPDATES

For the 25.2.0 release, the Application Security (Fortify) System Requirements is no longer a standalone document. The information has been included in the product user guide.

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 *OpenText™ Fortify WebInspect Agent Installation and Rulepack Kit Guide*.

Accessing Application Security Documentation

The Application Security (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 Application Security (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 25.2.0 must perform an offline activation of the LIM from the Admin page to enable SHA256.
- The *OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide* filename is listed as "lim-ugd-<version>.pdf" in the Related Documents topic in the dynamic and static Application Security Testing documentation. The actual filename is "LIM_Guide_25.2.0.pdf." The filename will be renamed in the 25.4.0 release.

OpenText ScanCentral SAST (Fortify ScanCentral SAST)

- The ScanCentral SAST client included in the OpenText™ Static Application Security Testing (Fortify Static Code Analyzer) installer is a newer version than the ScanCentral SAST Controller at time of release. OpenText recommends waiting until the ScanCentral SAST Controller version 25.2.0 is available before upgrading sensors to 25.2.0.

- If you are 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 24.4 (using the migration script and starting the Controller once), then upgrade to 25.2.0 (no need to run the migration script).

OpenText Static Application Security Testing (Fortify Static Code Analyzer)

- The ScanCentral SAST client included in the installer is a later version than the ScanCentral SAST Controller at the time of release. OpenText recommends waiting until the ScanCentral SAST Controller version 25.2.0 is available before upgrading sensors to 25.2.0.

OpenText Application Security (Fortify Software Security Center)

- 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, see the *Deploying Software Security Center* in Kubernetes on the Product Documentation website.
- Beginning in Software Security Center 25.2.0, Tomcat 10.1 is required. Review https://tomcat.apache.org/migration-10.html and https://tomcat.apache.org/migration-10.1.html for configuration changes when upgrading an existing installation using Tomcat 9.

USAGE NOTES FOR THIS RELEASE

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

Fortify License and Infrastructure Manager (LIM)

- Version 25.2.0 of the LIM and other Application Security (Fortify) products include both Secure Hash Algorithms (SHA) 1 and 256, which are used to verify communications between the LIM and other Application Security (Fortify) products. LIM version 25.2.0 can communicate with older versions of Application Security (Fortify) products that use only SHA1.

OpenText Static Application Security Testing (Fortify Static Code Analyzer)

- Version 25.2.0 updates the Security (default) and DevOps scan policies to reduce additional noise. Currently this is specified as "Risk", where an issue with low risk is defined as an issue with a low probability, unless it has a very high priority. Future releases will make this filter clearer and customizable.

OpenText Application Security (Fortify Software Security Center)

- Significant improvements were made to 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.
- 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 or 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)

- Software Security Center log rotation has been changed. When an Software Security Center log file reaches about 10 MB, it is rotated into logs/archive directory as `<original_basename>.<sequence_number>.log`. The higher sequence number designates an older log file. Logs from Software Security Center plugins are now stored along other Software Security Center log files into `ssc_plugins.log` file. Old rotated log files (stored in date-based logs subdirectory) need to be removed manually when appropriate.
- Software Security Center REST API specification switched from using Swagger 2 to OpenAPI 3. The Swagger 2 specification is still available on `${host.url}/api/v1/spec.json` URL, but it does not contain any REST API changes introduced after 24.4.0 release. The OpenAPI 3 specification is available at `${host.url}/api/v1/spec/openapi3.json` URL and is updated

with the latest API changes. Although Software Security Center 25.2.0 REST API is compatible with Software Security Center 24.4.0 REST API clients, an SDK generated from the Software Security Center OpenAPI 3 specification is not completely source code level compatible with an SDK generated from Software Security Center Swagger 2 specification.

- The fortifyclient command line tool underlying HTTP library was changed from OkHttp to Apache HttpClient library, and its REST API bindings are generated from the new Software Security Center Open API 3 specification. This might affect source-code compatibility of the fortifyclient source code provided in samples.
- REST API endpoint `/projectVersions/action/streamCustomTagAuditStates` now requires an admin account or a custom role with universal access.
- Issue IDs cannot have control characters. Any control characters in the issue data will be changed to spaces before being persisted.
- As of 25.2.0, Linux ARM architecture is supported for the Fortify Software Security Center Server.

OpenText 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 of OpenText SAST, there is a change in the Security (default) scan policy. Sensors based on this version may generate different results than previous versions because of this change.

OpenText ScanCentral DAST

- The DAST API v1 has been removed from the product.

- ScanCentral DAST 25.2.0 includes a new composite settings ZIP file that replaces the XML settings file format. ScanCentral DAST 25.2.0 no longer supports 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. Additionally, the following API endpoint has been 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 no longer generates scripts or compose files. Sample files with descriptions are provided instead.

KNOWN ISSUES

The following are known problems and limitations in Application Security (Fortify) Software 25.2.0. The problems are grouped according to the product area affected.

OpenText Application Security (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).

- In Software Security Center 24.4.0, an issue exists when trying to upload artifacts to empty PVs (those having no uploaded artifacts) migrated from previous versions to Software Security Center 24.4.0. These attempts end with artifacts in ERROR status and further attempts to delete these artifacts end with artifacts being stuck in DELETING status without a possibility to further maintain them from the UI. A fix for the empty PVs has been added to Software Security Center 25.2.0, but this fix is affecting only future artifact uploads. If artifacts with 'DELETING' status originated in 24.4.0 still exist in 25.2.0, they should be fixed manually by a simple SQL query given as a hot fix in 24.4.0.
- In Software Security Center 25.2.0, the "Analysis Type" was added in addition to the "Engine Type" for issues. This was a front end only change in 25.2.0 and therefore users will see some UI discrepancies with the Analysis Type. For example, if you Group by Analysis Type in the Audit page, you will still see the "Engine Type" labels on the grouped by rows.

OpenText ScanCentral SAST

- File path navigation in tools like Remediation plugins might be broken for some projects in certain languages (for example, JavaScript) due to the way SCA processes internal files. This might result in the `Src/` folder being prepended to file paths in FPR during ScanCentral remote translation and scan.
- OpenText Core SCA (Debricked) auto-installation might fail due to GitHub API restrictions. If it happens, it is recommended to manually install OpenText Core SCA and specify the path using the `debricked_cli_dir` property.
- Some ant patterns for the `–exclude/–include` flag might be expanded by the shell before reaching the application, causing ScanCentral CLI to malfunction. In case of issues, it is recommended to use known relative paths to files or folders without using ant patterns or to redesign the pattern to prevent shell expansion (for example, `.\**test\**` for Windows command line).

- The `setupworkerservice.bat` script for Windows improperly regenerates the existing `worker.properties` file. If properties were configured before creating a service, they would be lost. It is recommended to create the service, modify `worker.properties`, and then restart the service.
- If a Linux-specific project (one with files falling under Windows file path limitations such as case-insensitivity or prohibited characters, for example, Readme.md and README.md in the same folder or file names like 'test?', '.txt') is sent to the Windows sensor, the scan will fail. Such projects should be scanned using a sensor pool consisting exclusively of Linux sensors.
- If a project consists of subprojects (for example, multiple projects in a .NET solution), it is not possible to exclude an entire subproject from translation using the -exclude option (though it is possible to exclude files from the subproject). To exclude an entire subproject, it should be excluded from the build at the solution level.

OpenText Application Security Tools (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.

- In the Audit Workbench legacy report generator, older templates might not be displayed when loaded in version 25.2.0. To resolve this issue, add the attribute `showShortFileNames="false"` within the `'<IssueListing>'` tag in the corresponding `'<template_name>.xml'` files located in the `'<install_dir>/Core/config/reports'` directory.
- Following the rebranding of SCA (OpenText_SAST_Fortify_25.2.0), the tools are currently unable to automatically detect the SCA installation path. Users must manually provide the correct path to the rebranded SCA tool when prompted in 'AWB', 'Eclipse Analysis Plugin', 'IntelliJ Analysis Plugin' and 'Visual Studio complete extension'.

OpenText Static Application Security Testing (Fortify Static Code Analyzer)

- Analysing IaC languages and Solidity using the next-gen SAST engine cannot currently be accomplished with mobile build sessions. Users must either scan these projects locally or use remote translation and scan with ScanCentral SAST.

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

- Due to frequent base image updates caused by UBI security fixes, Application Security (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 the 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.

Fortify License and Infrastructure Manager (LIM)

- Starting in version 26.4.0, the LIM and other Application Security products will include only Secure Hash Algorithm (SHA) 256. After that, you must use a compatible version of the LIM to continue using Fortify product earlier than 26.4.0.

OpenText ScanCentral SAST

- Starting with version 25.4.0, the OpenText Static Application Security Testing (Fortify Static Code Analyzer) installer will no longer include the ScanCentral SAST sensor. Users will need to install the ScanCentral SAST sensor manually.
- In version 25.4.0, running the ScanCentral SAST Controller in standalone mode (without connecting to Software Security Center) will be deprecated. In future releases after 25.4.0, it will be required to run ScanCentral SAST Controller connected to an instance of Software Security Center.

OpenText Application Security (Fortify Software Security Center)

- WIE (Webinspect Enterprise) support will be deprecated in the Software Security Center 25.4.0 release. WIE (Webinspect Enterprise) will be removed from Fortify Software Security Center in 26.2.0.
- Out-of-order processing of artifacts support will be removed in the next release (25.4.0). This means that scans uploaded to Software Security Center out-of-order will not process the scan data. Audit changes will continue to process in Software Security Center regardless of what order the artifact is uploaded.
- ALM support will be deprecated in the Software Security Center 25.4.0 Release. ALM will be removed from Software Security Center in 26.2.0.
- The following API is now deprecated and will be removed in 25.4.0.

  ```
  /api/v1/userSession/state
  ```

OpenText Static Application Security Testing (Fortify Static Code Analyzer)

- The modular analysis feature is deprecated and will be removed from the product in a future release.

OpenText ScanCentral DAST

- 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.

OpenText Dynamic Application Security Testing (Fortify WebInspect)

- Version 25.4.0 will be the last release that includes Windows Docker images for OpenText DAST. 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, users must also use a LIM version 22.1.0 or later that supports usage of LIM REST APIs.
- 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.

OpenText Application Security Tools (Fortify Applications and Tools)

- The Custom Rules Editor might be redesigned and replaced with an alternate tool in a future release of OpenText Application Security Tools.

FEATURES NOT SUPPORTED IN THIS RELEASE

The following features are no longer supported.

OpenText Application Security (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.
- VSTSExtensionToken, which was deprecated in 24.2.0, is no longer supported. Already existing generated tokens of this type are revoked and removed during database migration. Use ScanCentralCtrlToken instead.
- Support for CAS and Kerberos Single Sign-on solutions was removed. If you previously configured one of these SSO services, you must reconfigure Software Security Center to use SAML 2.0, X.509, or HTTP Headers SSO before upgrading to this version. There is no automatic migration, and you might lose access to the Software Security Center otherwise.

- The option to enable Java Security Manager for BIRT reporting in Software Security Center ("Enhanced Security" option) was removed. Java Security Manger is deprecated in JDK 17 and subject for removal with no planned replacement in future JDK releases.
- The option to configure Conservative, Aggressive and Exclusive job execution strategies was removed. Automatic migration is not available. OpenText recommends using the default Flexible job strategy. Instructions for replicating behaviors of the deprecated strategies are in the user guide.
- Runtime-bridge utility JAR is no longer included in Fortify Software Security Center.

OpenText Static Application Security Testing (Fortify Static Code Analyzer)

- The `-apex` and `-apex-version` options are deprecated and will be removed in a future release.
- OpenText SAST no longer supports Visual Studio Web Site projects. Users must convert the Web Site projects to Web Application projects to ensure that OpenText SAST can scan them.

OpenText Application Security Tools (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.

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.