

OpenText™ Application Security Software

OpenText Application Security Software Release Notes 26.2.0

Version : 26.2

Table of Contents

1. OpenText Application Security Software Release Notes 26.2.0	1
--	---

1. OpenText Application Security Software Release Notes 26.2.0

Software Version: 26.2.0

Document Release Date: May 2026

Software Release Date: May 2026

This document provides installation and upgrade notes, known issues, and workarounds that apply to release 26.2.0 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 26.2.0*, which is available on the Product Documentation website.

FORTIFY DOCUMENTATION UPDATES

For the 26.2.0 release, OpenText Application Security Software (Fortify) System Requirements is now a standalone document. The System Requirements information has been removed from the product user guide.

The OpenText SAST System Requirements information has been excluded from the OpenText Application Security Software (Fortify) System Requirements and is available in the *OpenText Static Application Security Testing 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 for each product.

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

INSTALLATION AND UPGRADE NOTES

Complete instructions for installing Application Security (Fortify) Software products are provided in the documentation for each product.

OpenText ScanCentral SAST (Fortify ScanCentral SAST)

- Starting with version 26.2, the OpenText™ ScanCentral SAST Controller must be connected to an instance of Application Security.

OpenText Application Security (Fortify Software Security Center)

- Helm chart and values file for Application Security deployment to a Kubernetes Cluster are no longer located in the Application Security 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.
- Application Security requires Tomcat 10.1. 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)

- The LIM now supports PostgreSQL in addition to SQLite as a database option. This enhancement is available for both the desktop and container versions of the LIM.

OpenText Application Security (Fortify Software Security Center)

- Starting from version 26.2, the CE mark has been removed from the login, logout, masthead, and about pages.
- 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.

- To differentiate token authentication from user name or password authentication, Application Security uses separate events for token authentication on REST API endpoints:
 - WS_LOGIN_SUCCESS (Web Services Authentication Succeeded)
 - WS_LOGIN_WITH_NO_ROLE (Web Services authenticated user has no permission)
 - WS_LOGIN_FAILURE (Web Services Authentication Failed)
- SSC 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 SSC 25.4.0 REST API is compatible with SSC 24.4.0 REST API clients, an SDK generated from the SSC OpenAPI 3 specification is not fully source code level compatible with an SDK generated from SSC Swagger 2 specification.
- The issue-attachment-of-issue-controller REST endpoint will ignore the fileDocId value in an UPDATE request. This is to provide data consistency between attachments and their data.
- Verification of IdP metadata signatures using the IdP's public key (X.509 certificate) is now supported, improving security and integrity in SAML configurations.

OpenText Application Security Tools

- Starting from version 26.2, the CE mark has been removed from the login, logout, masthead, and about pages of Fortify Audit Workbench and Fortify Custom Rules Editor.

OpenText ScanCentral SAST

- In version 26.2, after setting up and using the components for the sensor auto-scaling feature, it is important that users must not use Kubernetes APIs to manipulate the components (for example, delete) while ScanCentral jobs are assigned, as this may cause instability and orphaned jobs. Use the ScanCentral SAST Controller API to cancel any jobs that are assigned and use the provided Helm charts to stop the ESF Adapter before modifying the components.

OpenText ScanCentral DAST

<To be added>.

Core SAST Aviator

- Version 26.2 introduces various functions to manage applications that have a number of open issues exceeding the available quota. For details, see the *OpenText™ Application Security Aviator for Vulnerability Remediation User Guide* on the Product Documentation website.
- Memory consumption when dealing with large FPRs has been substantially reduced.

KNOWN ISSUES

The following are known problems and limitations in Application Security (Fortify) Software 26.2.0. The problems are grouped according to the product area affected.

OpenText Application Security (Fortify Software Security Center)

- For successful integration with Fortify WebInspect Enterprise, Application Security must be deployed to a /ssc context. The context must be changed for the Application Security Kubernetes deployment, which uses the root context by default.
- The migration script downloaded from the maintenance page will be saved to a 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.

OpenText ScanCentral SAST

- Debricked auto-installation might fail due to GitHub API restrictions. If it happens, it is recommended to manually install Debricked and specify the path using the `debricked_cli_dir` property.
- The `setupworkerservice.bat` script for Windows improperly regenerates the existing `worker.properties` file. If properties were configured before creating a service, they will be lost. It is recommended to create the service, modify `worker.properties`, and then restart the service.

OpenText Application Security Tools (Fortify Applications and Tools)

- 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.

OpenText Static Application Security Testing (Fortify Static Code Analyzer)

- When scanning code using the AI-powered SAST, issues are not reported in file within directories indicating tests, examples or documentation, or in files that match common test naming patterns. This is currently not configurable.
- Analyzing Terraform, Solidity, and Bicep require downloading dependencies at scan-time if not provided manually. For optimal results, these languages should either be scanned locally or the scan machine should have a network connection to download dependencies.
- Some languages have scan-time dependencies that may make use across all platforms infeasible. This may have an effect when considering mobile build sessions or ScanCentral SAST sensors. Scan-time dependencies are specified in [Software Requirements](#)
- Some source files might be missing from the scan of an Xcode project if all targets in the project are not built for the same set of target architectures.

Workaround: If you encounter this problem, specify a single architecture for the build by adding the `-arch` option to the `xcodebuild` command that will be run by `sourceanalyzer`. You can also update the build configuration in the Xcode project or create a separate configuration to use for scanning and ensure that the target architecture(s) is the same for all targets.

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, OpenText no longer includes the minor version for UBI base images for the ScanCentral DAST, OAST, WebInspect, and 2FA Server products or product components.

FIXED ISSUES

OpenText Application Security Tools (Fortify Applications and Tools)

- 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 Visual Studio Extension, if the Application Security URL is not specified, and you attempt to upload an FPR or open a collaborative audit, Visual Studio might crash. Ensure to configure the Application Security URL prior to performing these actions.
- 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)

- Snippets are not included for ruby files when using AI-powered SAST though the source files are bundled in the FPR file.
- When using AI-powered SAST, Ruby source files are not counted in the number of analyzed `source file(s)` in the log file.

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, the LIM and other Application Security products will include only Secure Hash Algorithm (SHA) 256. After that time, if you continue using a Fortify product earlier than 26.4, then you must also use a compatible version of the LIM.

OpenText ScanCentral SAST

- ScanCentral SAST will be moving towards a standardized deployment using containers. The traditional software packages (Controller WAR file, Controller with bundled Tomcat) will be deprecated after the 27.2 release.

OpenText Application Security (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 Application Security.
- The CREATE method of the issue-attachment-of-issue-controller REST endpoint has been deprecated and disabled by default. It will be removed in a future release. It can be enabled in restApi.properties with the rest.enableLegacyCreateAttachmentEndpoint property.
- As Application Security moves towards a more standardized and consistent deployment using containers, the traditional software package (containing WAR file and seed bundles) will be deprecated after the 27.2 release.
- The fortifyclient cli tool has been deprecated and will be removed in the next release.
- The /issues/{parentId}/attachments POST endpoint is deprecated and will be removed next release.
- Password encoders support for LDAP authentication is obsolete and will be removed in the next release. Ensure you are only using the BIND_AUTHENTICATOR in the ldapserver configuration.

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.
- The `com.fortify.sca.FilterSet` property is deprecated and will be removed in a future release.
- The Intel-based macOS installer is deprecated and will be removed in a future release. The M-series (ARM) based installer will continue to be made available.

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.

- In version 26.2.0, the CE mark will be dropped from the product name.
- 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)

- Version 26.2 will be the last release that supports MacOS x64. Afterwards, only MacOS ARM (M-series chipset) will be supported.

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 Application Security. 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 Application Security after the migration. If you choose to continue using Bugzilla, in order to mitigate the issue, you must ensure that Application Security 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 Application Security.
- 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 Application Security 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 Application Security otherwise.
- The option to enable Java Security Manager for BIRT reporting in Application Security ("Enhanced Security" option) was removed. Java Security Manager is deprecated in JDK 17 and subject for removal with no direct 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 Application Security.
- ALM 12.5 Bug Tracker support will be deprecated beginning with the 25.4.0 release. Customers may continue to use ALM 12.5 Bug Tracker integration, but it will not be supported for defects or enhancements going forward.
- SQL Server 2017 is no longer supported.
- The `/api/v1/userSession/state` was deprecated in 25.2.0 and is now removed.

OpenText Static Application Security Testing (Fortify Static Code Analyzer)

Platform

- Microsoft Windows® version 10
- macOS® version 14
- IBM® AIX® version 7.1

Language

- .NET (Core) versions 2.x - 4.x
- .NET Framework versions 2.0 - 4.5
- C# version 5
- Swift versions 5.10 - 6.0

Build tool

- Ant version 1.9.x
- MSBuild version 14.x
- xcodebuild versions 15.3 - 15.4

Features

- Local analysis of Ruby has been removed. Use AI-powered SAST to analyze Ruby code.

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://portal.microfocus.com/>.

LEGAL NOTICES

Copyright 2026 Open Text

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.



© Copyright 2026 Open Text

For more info, visit <https://docs.microfocus.com>
