OpenText™ Application Security Software Release Notes 26.4.0

OpenText™ Application Security (Fortify) Software Release Notes
Version 26.4

PDF Generated on November 11, 2026

© Copyright 2026 Open Text

Table of Contents

OpenText™ Application Security (Fortify) Software Release Notes 3

OpenText™ Application Security (Fortify) Software Release Notes

Software Version: 26.4.0

Document Release Date: November 2026
Software Release Date: November 2026

This document provides installation and upgrade notes, known issues, and workarounds that apply to release 26.4.0 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 26.4.0*, which is available on the Product Documentation website.

FORTIFY DOCUMENTATION UPDATES

The *Fortify System Requirements* document no longer includes system requirements for SAST, LIM, and WebInspect. This information is now available in the documentation for each respective product.

The link to the Fortify Audit Assistant On-Premises documentation has been updated. 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 content from these guides has been consolidated into 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.

Fortify License and Infrastructure Manager (LIM)

- The LIM The License and Infrastructure Manager (LIM) now supports the Secure Hash Algorithm (SHA) 256. Offline customers upgrading to version 25.2 must perform an offline activation of LIM from the **Admin** page to enable SHA-256 support.
- The **Related Documents** topic in the DAST and SAST documentation incorrectly lists the *OpenText Fortify License and Infrastructure Manager Installation and Usage Guide* file name as `lim-ugd-<version>.pdf`. The correct file name is `LIM_Guide_25.4.0.pdf`. This file name will be renamed in a future release.

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.

OpenText Application Security Tools (Fortify Applications and Tools)

- **Bundled FCLI Support:** Starting with **version 26.4**, `FCLI.exe` is included with OpenText Application Security Tools. The installer provides an option to download and install the latest FCLI release.

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)

- LIM 25.4 and other Fortify products support both SHA-1 and SHA-256 for verifying communications between the LIM and other Fortify products. LIM 25.4 can communicate with earlier versions of Fortify products that support only SHA-1.

OpenText Application Security (Fortify Software Security Center)

- 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 `withoutCount` query parameter was added to paginated REST API listing endpoints, with a default value of `false`. The parameter can be used to disable computing the total object count for the `count` response field. It was added primarily to improve performance for the `/api/v1/activityFeedEvents` endpoint. Setting the parameter to `true` might improve performance for some other supported endpoints, although performance improvements are not expected in all cases. The addition of this query parameter might require changes to code that uses Swagger/OpenAPI code generation to create API SDKs. This applies at least to API SDKs generated for Java.
- To differentiate token authentication from username/password authentication, Application Security uses 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 permissions)
- The `issue-attachment-of-issue-controller` REST endpoint ignores the `fileDocId` value in an UPDATE request. This provides data consistency between attachments and their data.
- The `/issues/{parentId}/attachments` POST endpoint has been removed and is no longer supported.
- The CREATE method of the `issue-attachment-of-issue-controller` REST endpoint has been removed and is no longer supported.
- LDAP authentication using a password comparator is obsolete and is no longer supported. Ensure that you use only `BIND_AUTHENTICATOR` in the `ldapserver` configuration.
- The **Manage Application Version** access permission requires the **View Roles** and **View Users** permissions, and this requirement is now enforced in the Application Security user interface.
- Allow-list the private CIDR range(s) that contain your webhook targets by setting the following property in `app.properties` and restarting Application Security, as shown in the following example:
  `webhooks.sender.ssrf.allowedCidrRanges=10.0.0.0/8,192.168.0.0/16`
- The following property can be set in `app.properties` to restrict whether a user who uploads a scan result (FPR) can also approve that scan for processing:
  `artifact.approver.cannot.be.uploader` defaults to `false` (legacy behavior that allows the uploader to approve the scan). The **Approve Analysis Results Upload** permission is still required.
- You can use the following property in **app.properties** to control whether the user who uploads a scan result (an FPR file) can also approve the scan for processing:
  `artifact.approver.cannot.be.uploader`
  The property defaults to **false** (legacy behavior), which allows the uploader to approve the scan. The **Approve analysis results upload** permission is still required.

- Defensive formula sanitization for CSV exports is now stricter by default. The `export.enhanced.sanitization.enable` property now defaults to `true`. Set the property to `false` to retain the legacy behavior, which sanitizes only values that begin with `=`.
- Application Security 26.4 includes compatibility handling for older Black Duck parser plugin versions that contain malformed Issue View Template definitions. While these older plugin versions remain supported and continue to function, OpenText recommends upgrading to the latest Black Duck parser plugin release. The latest plugin versions contain corrected template definitions and should be used to ensure long-term compatibility and supportability.
- The granularity of the scan engine version comparison used during FPR upload validation is now configurable for greater flexibility.
  `scan.engine.version.full.check`
  - `false` (default): Compares only the **major.minor** version. For example, **24.2.0.0150** and **24.2.9.9999** are treated as the same engine version.
  - `true`: Compares the full engine version (**major.minor.patch.build**), preserving the legacy behavior for backward compatibility.

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

- The DAST API v1 has been removed from the product.
- ScanCentral DAST 25.2 includes a new composite settings ZIP file that replaces the XML settings file format. ScanCentral DAST 25.2 no longer supports downloading settings files in XML format. Settings files downloaded from the ScanCentral DAST UI are provided in the new composite settings ZIP file format. Additionally, the following API endpoint has also been disabled:
  `/api/v<version:apiVersion>/application-version-scan-settings/<scanSettingsId:int>/download-scan-settings-xml`
- Starting from version 25.2, the ScanCentral DAST Configuration Tool CLI no longer generates scripts or Compose files. Instead, sample files with descriptions are provided.

Core SAST Aviator

- **LLM-Based Auditing for DAST Findings -** Fortify Remediation Aviator 26.4 introduces support for LLM-based auditing of DAST findings, including bulk auditing. For more information, refer to the User Guide.
- **Enhanced Aviator Connection Diagnostics for Enterprise Proxy Environments -** New connection diagnostics provide stage-specific results to help identify and troubleshoot Aviator connectivity issues in enterprise proxy environments.
- **Local FPR File Support for Aviator Remediation Commands -** Aviator remediation commands now support local FPR files, allowing users to reuse previously downloaded FPR files across multiple remediation runs.
- **Improved Auto-Remediation and Preview Experience -** This release includes various improvements to automated remediation workflows and the review of remediation changes in the preview mode. For more information, refer to the User Guide.

KNOWN ISSUES

The following are known problems and limitations in Application Security (Fortify) Software 26.4.0. 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.
- Application Security 26.4 running on Java 25 uses new Java XML/SAX security limits. The following default limits are unchanged in the Application Security distribution:
  - `-Djdk.xml.maxGeneralEntitySizeLimit=100000` : Maximum escaped characters in a single XML entity
  - `-Djdk.xml.totalEntitySizeLimit=100000` : Maximum escaped characters across all XML entities in a document
  - `-Djdk.xml.entityExpansionLimit=1500` : Maximum XML entity expansions

  If an FPR upload fails when Application Security is running on Tomcat with Java 25 and reports a `JAXP00010003` , `JAXP00010004` , or `JAXP00010001` parser error, the FPR content might exceed the default Java XML security limits. To resolve the issue, reduce or simplify the FPR XML complexity, or increase the applicable Java XML security limit at runtime using one or more of the following parameters:
  - `-Djdk.xml.maxGeneralEntitySizeLimit`
  - `-Djdk.xml.totalEntitySizeLimit`
  - `-Djdk.xml.entityExpansionLimit`

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.
- ScanCentral SAST scans do not work properly when run from a project which contain spaces in the path.

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 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)

Audit Workbench no longer repeatedly prompts for Fortify SSC sign-in when users select vulnerabilities in an FPR that is not associated with the configured SSC. The sign-in prompt is displayed only once.

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 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.
- Removal of the SOAP messaging protocol from Fortify WebInspect has been postponed until version 25.2. After upgrading to Fortify WebInspect version 25.2, you must also use a LIM version 22.1 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.

OpenText Application Security Tools (Fortify Applications and Tools)

- In the 27.2 release, fortifyclient will be removed from the OpenText Application Security Tools installer.
- **Bundled FCLI Support:** Starting with **version 26.4**, *FCLI.exe* is included with OpenText Application Security Tools. The installer provides an option to download and install the latest FCLI release.

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.

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