

OpenText™ Fortify Remediation Aviator

Release Notes (26.4)

Version 26.4

Table of Contents

Release Notes (26.4)	3
1 Fortify product name changes	3
2 New features	3

Release Notes (26.4)

This document provides the new features, installation and upgrade notes, known issues, and workarounds that apply to release 26.4 of OpenText™ Fortify Remediation Aviator.

This information is not available elsewhere in the product documentation. The user guides for this product are available on the Product Documentation website:

<https://www.microfocus.com/documentation/fortify-static-code-analyzer-and-tools/>

1. Fortify product name changes

OpenText is in the process of changing the following product names:

Previous name	New name
OpenText™ Static Application Security Testing (OpenText SAST)	OpenText™ Fortify Static Application Security Testing (OpenText Fortify SAST)
Fortify Software Security Center	OpenText™ Application Security
Fortify WebInspect	OpenText™ Fortify Dynamic Application Security Testing (OpenText Fortify DAST)
OpenText™ Core Application Security	OpenText™ Fortify on Demand
OpenText™ Core Software Composition Analysis (OpenText Core SCA)	OpenText™ Fortify Software Composition Analysis (OpenText Fortify SCA)
OpenText™ Application Security Aviator	OpenText™ Fortify Remediation Aviator
Fortify Applications and Tools	OpenText™ Application Security Tools

The product names have changed on product splash pages, mastheads, login pages, and other places where the product is identified. The name changes are intended to clarify product functionality and to better align the Fortify Software products with OpenText. In some cases, such as on the documentation title page, the old name might temporarily be included in parenthesis. You can expect to see more changes in future product releases.

2. New features

Languages

- All categories for HTML, Ruby, Solidity, Bicep, Terraform, YAML, JSON, Dart, Flutter, Objective-C++, and Objective-C are now supported with automatic suppression.

New features/updates

- Added category combinations for DAST that support automatic suppression.
- Fortify Remediation Aviator now supports LLM-based auditing of DAST findings. For each eligible finding in a DAST FPR, Fortify Remediation Aviator determines whether the finding is a true positive or false positive and writes the result back to the FPR in an OpenText Application Security compatible format. The same quota and entitlement

model used for SAST auditing applies.

Also supports bulk DAST auditing for application versions from a single command.

- Fortify Remediation Aviator CLI now supports DAST audit processing for Fortify on Demand. Fortify on Demand passes a DAST FPR input path, an output path, and the available quota to the CLI.
- `fcli remediation` now applies fixes deterministically with explicit outcomes for every remediation. Enhancements include:
 - Normalization of proposed fixes
 - Canonical and legacy-compatible hash validation
 - Detection of identical and competing fixes
- FCLI now supports iterative OpenText Application Security remediation workflows through the `--force-reaudit` option and unique anchor-match validation. Use `--force-reaudit` to resubmit previously audited unresolved issues after code changes and a new SAST scan.
- `fcli aviator ssc apply-remediations` now handles source files with unknown or non-UTF-8 encodings using the standard OpenText Fortify SAST encoding strategy. Customers can specify an additional encoding parameter if required. Source-file processing failures are reported with the correct context.
- Fortify Remediation Aviator now preserves the remaining application quota when applications are deleted. The entitlement associated with the deleted application becomes available for other applications to consume.
- `fcli` now provides a dedicated Fortify Remediation Aviator connection diagnostics mode that checks the following in sequence:
 - Endpoint configuration
 - DNS resolution
 - TCP connectivity
 - TLS handshake
 - gRPC request and response reachability
 - Optional token validation

The diagnostics output provides guidance for failures, distinguishes successful TLS establishment from gRPC response receipt, and supports machine-readable output for support scenarios.

- `fcli aviator ssc apply-remediations` and `fcli aviator fod apply-remediations` now support filtering remediation by one or more comma-separated issue identifiers and a preview option so users can review remediations before they apply them.
- `fcli aviator ssc apply-remediations` and `fcli fod aviator apply-remediations` now support loading remediations from a local FPR file.
 - Uses the supplied local FPR and does not download an artifact from OpenText Application Security or Fortify on Demand.
 - Validates that the local FPR exists, can be read, and is valid before processing starts, and returns a clear error when validation fails.
 - Preserves download-based behavior when no local FPR path is supplied.

Installation and upgrade notes

- `fcli` v3.28.0 or later



© Copyright 2026 Open Text

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