OpenText™ Fortify on Demand

Release Notes (26.3.0)

Version 26.3

PDF Generated on September 10, 2026

Table of Contents

Release Notes (26.3.0)

This document provides the new features, installation and upgrade notes, known issues, and workarounds that apply to release 26.3.0 of OpenText™ Fortify on Demand (FoD).
This information is not available elsewhere in the product documentation. The user guides for this product are available on the Product Documentation website:
OpenText Fortify on Demand (FoD) - Documentation | Micro Focus

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 SAST
Fortify Software Security Center	OpenText™ Application Security
Fortify WebInspect	OpenText™ 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. Engine and rulepack updates

OpenText Fortify on Demand 26.3.0 includes the following engine and rulepack versions:

- **Fortify Software Security Content 26.2.0:**
  OpenText Fortify on Demand implements Fortify Software Security Content 26.2. For more information, see OpenText Application Security Content (Fortify) Update 26.2.
- **OpenText Static Application Security Test 26.2.0:**
  OpenText Fortify on Demand implements OpenText SAST (Fortify Static Code Analyzer) version 26.2.
- **OpenText Dynamic Application Security Test (DAST) 26.2:**
  OpenText Fortify on Demand implements OpenText Dynamic Application Security Testing version 26.2 for dynamic application scanning.

3. New features

Introducing auto-scaling scanner architecture

Fortify on Demand introduces a cloud-native auto-scaling scanner architecture that dynamically adjusts scanning resources based on demand, improves workload orchestration, and increases scan reliability through automated recovery capabilities.

With the core architecture now complete, a phased rollout is underway in controlled customer batches. Phase 1 focuses on SAST workloads and supports:
- ScanCentral-packaged payloads, excluding .NET and .NET Framework applications
- Non-ScanCentral-packaged payloads for JavaScript (JS), TypeScript (TS), HTML, and Infrastructure as Code (IaC)

Eligible customers automatically benefit from improved scan stability, enhanced resiliency, and more efficient resource utilization, with no changes required to existing scan workflows. Support for additional technology stacks and payload types will be introduced in future rollout phases. For more information, see Configuring a Static Scan.

New Program and Risk Exposure Dashboards

Fortify on Demand now includes enhanced Program and Risk Exposure Dashboards that provide a comprehensive view of application security posture, scan adoption, risk exposure, and entitlement utilization across the organization.

These dashboards give security leaders, compliance teams, DevSecOps teams, and application owners the visibility needed to measure security program effectiveness, prioritize remediation efforts, and reduce organizational risk. For more information, see Dashboards.

Scan Policy Selection for SAST Scans

Fortify on Demand now supports scan policy selection for SAST scans, enabling organizations to choose the policy to be used during analysis. This enhancement provides greater control over scan results while helping align security testing with development workflows and risk management objectives.

Scan policies can be configured through both the Fortify on Demand user interface and APIs. Available policies include:
- Security
- Classic
- DevOps
- FoD Legacy (default, preserving the existing Fortify on Demand scanning experience and backward compatibility).

For more information, see Configuring a Static Scan and Viewing Release Scans.

Enhanced Debricked Open Source Scan Results

Fortify on Demand now surfaces malware indicators and known exploited vulnerability (KEV) information from Debricked scan results, providing greater visibility into open-source risk.

These enhancements help Security and AppSec teams identify, prioritize, and remediate high-risk open-source findings directly within Fortify on Demand.

For more information, see Open Source Software Composition Analysis and Filtering and Grouping the Issues Page.

Concurrent Dynamic Scanning for Applications

Fortify on Demand now supports concurrent Dynamic scans, allowing organizations to run multiple Dynamic scans simultaneously across different releases of the same application. Administrators can configure the maximum number of concurrent Dynamic scans allowed per application through a new tenant-level setting, enabling teams to test parallel development streams more efficiently and reduce scan scheduling bottlenecks. This capability applies to all Dynamic assessment types except Dynamic Automated. For more information, see Configuring a Dynamic Scan.

Manually Start Dynamic Subscriptions

Fortify on Demand now offers the ability for authorized users to better manage their Dynamic subscription entitlements by starting subscriptions directly from the Dynamic Scan Settings page. This eliminates the need for placeholder scans,

simplifies entitlement consumption, accelerates application onboarding and CI/CD setup, and provides greater control and visibility into entitlement usage. For more information, see Viewing Application Scans.

Mobile+ Site Tree Download Support

Fortify on Demand now provides enhanced visibility into application coverage during Mobile+ assessments by enabling users to download the site tree discovered during manual testing activities. This capability helps teams better understand tested application areas and assessment coverage. For more information, see Editing Mobile Scan Settings for an Ongoing Scan.

Global Filtering Enhancements

This release introduces new visibility and filtering enhancements across the Your Applications, Your Releases, and Your Scans pages. Users can now view, sort, and filter releases and scans by ownership and initiator details, improving accountability and operational visibility. In addition, the Applications page now includes Aviator-related filtering criteria, making it easier to identify applications based on their Aviator enablement and status. For more information, see Filtering Your Applications Page, Filtering Your Releases Page, and Filtering Your Scans page.

Reporting Enhancements

This release introduces reporting enhancements that improve automation and visibility across Fortify on Demand security reporting workflows.

Key updates include:
- Automatic generation of OSS Components reports upon Open Source scan completion, streamlining open-source risk reporting and compliance processes
- Reports generated through Fortify on Demand APIs are now visible in the Tenant Portal Reports tab, providing a centralized view of all reports regardless of creation method. For more information, see Reports, Viewing Release Reports, and Scheduling Auto-Generated Reports.

Data Export Enhancements

This release expands issue data exports with additional visibility into vulnerability history and open-source component origins.

Key updates include:
- Audit History can now be exported for individual issues, enabling reviewers to track status changes and audit events directly from exported data
- File Location information is now included for applicable Sonatype findings, helping teams identify where vulnerable components exist within their codebase

For more information, see Data Exports.

Audit template updates

This release extends audit template capabilities by adding support for the Info and Best Practice severity categories.

Security teams can now configure audit rules based on these severity levels in both Global Audit Templates and Application Audit Templates, enabling more comprehensive and consistent issue management across Static, Dynamic, Mobile, and Open Source scan results.

For more information, see Creating a Global Audit Template and Creating an Application Audit Template.

API updates

The following updates have been made to the OpenText Fortify on Demand API.

DAST API Support for Two-Factor Authentication (2FA)

The Fortify on Demand DAST API now supports Two-Factor Authentication (2FA), enabling the configuration and automation of Dynamic scans for applications protected by modern authentication mechanisms.

Supported authentication methods include:
- Email-based 2FA
- TOTP (Time-Based One-Time Password)

The API also supports TOTP QR code processing and secure credential management. These enhancements simplify automation for applications requiring multi-factor authentication while maintaining secure handling of authentication data and full backward compatibility with existing API workflows.

For more information, see Configuring a Dynamic Scan and Viewing API Documentation through API Explorer.

4. Known Issues

Issues with PDF outputs

Description

The customer-facing PDF documents of OpenText Fortify on Demand (FoD) contains cross-reference links that do not navigate to the intended section or page. Users relying on these links to quickly access referenced content may need to locate the information in the document manually.

Workaround

Use the search feature in the PDF viewer to locate the referenced section manually.

Status

The issue is under investigation.

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