Application Security Software

Document Release Date: May 2025

# What’s New in Application Security (Fortify) Software 25.2.0

## May 2025

This release of Application Security (Fortify) Software includes the following new functions and features.

## OpenText™ Application Security (Fortify Software Security Center)

The following features have been added to OpenText™ Application Security.

**System requirements**

- TomCat 10.1
- Dropping support for SQL Server 2017
- Linux ARM
- Kubernetes 1.30, 1.31, and 1.32 support
- Helm 3.16 and 3.17 support

**Modern Applications view**

Improvements to the Applications page and navigation options when viewing content in the UI.

**ScanCentral SAST scan requests**

Improved display and filtering options of the ScanCentral SAST scan requests.

### Accessibility improvements

Accessibility improvements in Contrast and Non-text Contrast categories to reach the WCAG Level AA compliance.

### Renaming Fortify Software Security Center to OpenText Application Security

Fortify Software Security Center (SSC) will be changing the name of the product to OpenText Application Security. In this initial phase, you will see the login, logout, masthead, and about pages with the new name. You will see some changes and references to the new name in documentation, but not everywhere. Over the next several releases, the name change will continue to propagate through all areas of the product. You will continue to see references to Fortify and Software Security Center and some references to Application Security Center in areas of the product. All of these are referencing Fortify Software Security Center (SSC).

### FPR processing rules – File and LOC counts

You can separately apply FPR processing rules to increase or decrease the file count or lines of code by a certain percentage . The percentage is still set globally in the server configuration file. Additionally, use the new configuration settings to define a minimal number of files and/or a minimum lines of code to apply the new rules on an application version.

### Analysis type

The following analysis types are introduced to represent Software Security Center Engine Types.

- OpenText™ Static Application Security Testing (Formerly Static Code Analyzer)
- OpenText™ DAST (Formerly WebInspect)

### Configurations warnings

Configuration warnings have been added to several administrator settings to emphasize the impact of configuration changes to the product. Changes such as Single Sign-on, SSO Options, ScanCentral SAST now have additional warnings on the configuration pages. When choosing to save a change there is an additional pop-up warning that the user must accept to save the changes.

# OpenText™ ScanCentral SAST

The following features have been added to Fortify ScanCentral SAST.

**Email notification enhancements**

- You can include Job status in the email subject.
  - Use the `include_job_status_in_email` property in the `config.properties`
  - Set to `false` if using email “conversations” where emails are grouped by subject (for example, Gmail) to see all emails for a Job in the same grouping
- You can add up to 100 email addresses using the command line.
- Job Token, Build ID, Application Name, Version Name, AppVersion ID, SSC URL are included in the email body.

**Controller logging options**

You can configure the Controller logging by setting environment variables on the system where you installed the Controller.

**Sensor pool name**

Specify the sensor pool name when submitting a scan request.

**Include Files in the Package**

Use the new command line option `-include` to specify the files that you want to include in the generated ScanCentral SAST package.

**Helm Chart and Docker Images**

- Support for TLS for secure connections (required)
- Improved documentation
- DB Migration container added to Iron Bank

**ScanCentral client**

- Use the `-skipBuild` option in the scan request command to prevent ScanCentral SAST from automatically restoring dependencies. This option is available for Go, JavaScript/TypeScript, PHP, and Python projects.
- Support for `pnpm` package manager.

# OpenText™ Static Application Security Testing (Fortify Static Code Analyzer)

The following features have been added to OpenText™ Static Application Security Testing.

**Features/Updates**

- Added support for Jupyter notebooks for Python translations.

# OpenText™ Application Security Tools (Fortify Static Code Analyzer Tools)

The following features have been added to Fortify Static Code Analyzer tools.

**New report template versions**

- PCI DSS 4.0.1
- MISRA C 2023
- DISA STIG 6.1
- CWE Top 25 2024

# OpenText™ ScanCentral DAST

The following features have been added to OpenText ScanCentral DAST.

**TLS authentication**

ScanCentral DAST now supports TLS authentication between the ScanCentral DAST components.

**Advanced scan settings**

Most of the Advanced scan settings from WebInspect have been added to ScanCentral DAST. You can see and configure these additional settings in the Advanced view in the scan wizards and by way of the API.

**Log table**

A new Logs table displays the OpenText DAST sensor scan log for the selected scan.

**Multiple policy selection**

Scan settings now support selecting multiple policies to use while conducting a scan.

**WebInspect settings status**

The new WebInspect Settings Status column in the Settings List view Indicates whether composite settings have been generated for downloading and using in OpenText DAST (Fortify WebInspect).

**New key store type**

Key stores now support a Password type for key store entries.

**Sensor type column**

The Sensors view content with details about Sensor Type column that indicates whether the sensor is fixed or auto scaled.

**Page navigation enhancements**

Enhancements have been made to the page navigation options when viewing content on multiple pages in the UI.

**Event-based Web Macro Recorder**

The Event-based Web Macro Recorder Mac version now includes the following new features:

- A main application window that provides options for recording Login, Workflow, and Workflow with Login macros, and for accessing recently edited macros
- A Web Macro Recorder widget that provides a quick launch method to record a web macro
- Support for the macOS QuickLook feature to view information about a web macro file without actually opening the Web Macro Recorder

The Event-based Web Macro Recorder now enables you to record a login macro using IMAP multi-factor authentication with OAuth2.

## OpenText™ DAST (Fortify WebInspect)

The following features have been added to OpenText DAST.

**Multiple policy selection**

The scan wizards, wi.exe, and scan settings now allow you to select multiple policies for use in a single scan.

**New user agents**

New user agents are available in the default scan settings.

**Composite settings**

OpenText DAST now offers the option of using composite settings that consist of a JSON version of the scan settings packaged in a ZIP file with any binary files required for the scan, such as macros, client certificates, custom policies, and so forth. An option to enable composite settings is available in the **Application settings > General** tab.

**Event-based Web Macro Recorder**

The Event-based Web Macro Recorder Mac version now includes the following new features:

- A main application window that provides options for recording Login, Workflow, and Workflow with Login macros, and for accessing recently edited macros
- A Web Macro Recorder widget that provides a quick launch method to record a web macro
- Support for the macOS QuickLook feature to view information about a web macro file without actually opening the Web Macro Recorder

The Event-based Web Macro Recorder now enables you to record a login macro using IMAP multi-factor authentication with OAuth2.

# What’s New in Fortify Software 24.4.0

## October 2024

This release of Fortify Software includes the following new functions and features.

## Fortify Software Security Center

The following features have been added to Fortify Software Security Center.

**Technology Preview: Magellan BI and Reporting Dashboards**

This release includes a preview of upcoming support for the inclusion of OpenText Magellan BI and Reporting dashboards in Fortify Software Security Center. The Magellan BI and Reporting dashboards provide a comprehensive application security program overview, insights into important vulnerability metrics, and consistent dashboard views among the Fortify product Suite. If you are interested in previewing the upcoming Magellan dashboard integration, contact Customer Support for the software and support required to run the Technology Preview.

**Audit Issue History Tracking**

- You can track changes in the attributes of an issue as you upload new scans for an audit. The issue history includes all attributes that Fortify Software Security Center extracts from uploaded scans that can be searched or filtered on the audit page.

### ScanCentral SAST Controller role

- The ScanCentral SAST Controller role is a new pre-configured role. This role is Intended for use only when configuring a Fortify ScanCentral SAST Controller. It allows users who are permitted to run scans but do not have upload analysis result permissions to upload scans.

### Kubernetes support

- Support added for Kubernetes versions 1.30 and 1.
- Support added for Helm command-line tool versions 3.15 and 3.16.

# Fortify ScanCentral SAST

The following features have been added to Fortify ScanCentral SAST.

**Uploading analysis results to Fortify Software Security Center**

- You can configure the ScanCentral SAST Controller with a ScanCentral SAST Controller service account created in Fortify Software Security Center. This enables to upload the scan results to Fortify Software Security Center using the Controller service account. In this case, your Software Security Center user accounts do not require the upload analysis results permission.
- The start command -uptoken option is no longer required to upload scan results to Fortify Software Security Center if you specify the -sscurl and -ssctoken option pair.

**ScanCentral client**

- You can add JVM system and ScanCentral SAST properties (for clients and sensors) to the ScanCentral client commands by adding the -D option to the SCANCENTRAL_VM_OPTS environment variable. You can add JVM system properties to the environment variable for use by the PackageScanner tool.
- You can retrieve your package (job file) from the Controller using the retrieve command --job-file option.
- The client start command -sargs option accepts the Fortify Static Code Analyzer -bin option.
- The client start command -targs option accepts the Fortify Static Code Analyzer -gotags option.
- When packaging PHP projects that use Composer for dependency management, the ScanCentral client will automatically restore the dependencies prior to generating the package.
- Support packaging Maven projects that use the `-Dmaven.repo.local` or `-Dsettings.localRepository` properties to configure a non-default local repository location.

**Updated build tool support**

- Support for Gradle 8.7 - 8.10

**ScanCentral SAST containers**

- New ScanCentral SAST Windows Sensor container with Windows Server 2022 as a base image
- New database migration container to migrate the ScanCentral SAST Controller database when upgrading

# Fortify Static Code Analyzer

The following features have been added to Fortify Static Code Analyzer.

**Platforms**

- Linux on ARM support
- IBM AIX 7.3

**Languages**

- .NET (Core) 9.x
- ABAP 7.x
- Angular 17
- Apex 61
- C# 13
- Go 1.23
- Kotlin 2.0
- PL/SQL 10, 11, 12, 18, 19, 21, and 23
- TypeScript 5.3 and 5.4

**Build tools**

- Bazel 7.x
- Gradle 8.5
- MSBuild 17.11
- MSBuild and Bicep support on .NET 8

**Platforms and architectures**

- Added support for IBM AIX 7.3.

**Features/Updates**

- Updated the scan policies with the ability to exclude dataflow issues based on taint flags
- Added support for Go build tags with the `-gotags` command-line option
- Added support for Flask framework and Jinja2 templates

# Fortify Static Code Analyzer Tools

The following features have been added to Fortify Static Code Analyzer tools.

**Secure code plugins**

- Support for Eclipse 2024-06
- Support for IntelliJ IDEA 2024.2
- Support for Android Studio 2023.3 and 2024.1
- Support for Azure DevOps Server 2022

# Fortify ScanCentral DAST

The following features have been added to ScanCentral DAST.

**Scan Details now has Create By**

The scan details panel now displays the user that created/imported the scan.

**New REST endpoint to view messages**

SC DAST has added an endpoint to retrieve the polling messages that occur in the product. These are primarily the message that the global service is processing from the sensors.

**Linux containers now on UBI9**

The SC DAST containers on Linux is now on the RedHat UBI9 with .NET 8.

# Fortify WebInspect

The following features have been added to WebInspect.

**WebInspect CLI & API**

Support has been added for using an external SQL Server database when using either the WebInspect CLI or the WebInspect API.

**Expanded URL field**

URL field has been expanded for API scans using a postman collection. This allows the user to view the authentication endpoints and proceed with a dynamic token strategy.

**HAR improvements**

Updates to the HAR parser allows for a greater number of formats from different browsers.

**New logging option**

New environment variable for logging to stderr output.

**Linux containers now on UBI9**

The WebInspect container on Linux is now on the RedHat UBI9 with .NET 8.

# Contacting Customer Support

Visit the Support website to:

- Manage licenses and entitlements
- Create and manage technical assistance requests
- Browse documentation and knowledge articles
- Download software
- Explore the Community

https://www.microfocus.com/support

We Welcome Your Feedback

If you have comments or suggestions about the documentation, you can send these to the documentation team at fortifydocteam@opentext.com. Please use the subject line “Feedback on <Document_Title> <Product_Version>.” We appreciate your feedback!

# What’s New in Fortify Software 24.2.0

## May 2024

This release of Fortify Software includes the following new functions and features.

## Fortify Software Security Center

The following features have been added to Fortify Software Security Center.

**Data Retention**

Administrators can define time period for retaining application version artifacts.

**Customizable UI Theme**

You can now set the UI theme to dark, light, or automatic.

**Customized BIRT Reports**

- Generate and download customized BIRT reports in XLSX format.
- Supports BIRT Report Designer 4.14.0

**Syncronize Audit History Changes in Fortify ScanCentral DAST using Kafka**

You can set up Kafka to synchronize audit history changes for suppressed issues, priority override, and analysis tag with Fortify ScanCentral DAST.

**fortfyclient Timeouts**

Set up timeouts for connect, read, and write for fortifyclient.

**Kubernetes support**

1.29

**Helm support**

**3.13 and 3.14**

**Updated LOC (lines of code) calculation**

To better align with the LOC count shown by code editors, Fortify Static Code Analyzer now reports the total number of lines of code, including blank lines and comments. Due to this change, when you upload an artifact created with Fortify Static Code Analyzer 24.2.0 (or later) to an SSC application version that already contains artifacts generated by earlier versions of Fortify Static Code Analyzer, a one-time approval may be required if the following processing rule is enabled: `Require approval if line count differs by more than 10%`. Once a 24.2.0 artifact has been approved in an application version, subsequent 24.2.0 uploads to that application version will no longer trigger the processing rule unless the LOC count changes due to significant code changes or changes in the scan setup.

# Fortify ScanCentral SAST

The following features have been added to Fortify ScanCentral SAST.

**Sensor Version Support**

Scan requests initiated from older clients can be assigned and processed by newer sensor versions.

**Encoded Tokens**

Added support for encoded tokens (decoded tokens are deprecated).

**ScanCentral SAST Client**

- Ability to use the Debricked CLI for open source software composition analysis (for use with Fortify on Demand only).
- Simplified commands by automatically detecting `requirements.txt` for Python projects, the PHP version for PHP projects, and setting a default value for package name.

**ScanCentral Controller**

You can configure the Controller to disallow queuing multiple scan requests that are uploaded to the same application version. If enabled, newer scan requests will replace the one that is in the queue while keeping its priority. It can be overridden with an option for individual scan requests.

**Updated Build Tool Support**

- Support for Gradle 8.6
- Support for dotnet 8.0
- Support for MSBuild 17.9

# Fortify Static Code Analyzer

The following features have been added to Fortify Static Code Analyzer.

**Platforms**

- macOS 14 support

**Languages**

- Angular 16.1 and 16.2
- Apex 59 and 60
- C23
- Dart 3.1
- Django 5.0
- Flutter 3.13
- Go 1.21 and 1.22
- Java 21
- Kotlin 1.9
- PHP 8.3
- Scala 3, versions 3.3-3.4
- Swift 5.10
- TypeScript 5.1 and 5.2
- Visual Basic (VB.NET) 16.9

**Compilers**

- gcc 13
- g++ 13
- Swiftc 5.9.2, 5.10

**Build tools**

- Bazel 6.4.0
- CMake 3.23.3 and later
- MSBuild 17.9
- xcodebuild 15.3

**Features/Updates**

- ARM JSON Templates (IaC)
- AWS CloudFormation (IaC)
- Scanning .NET requires .NET SDK 8.0.
- The default python version is now 3.
- The default scan policy has changed from classic to security. The security scan policy excludes issues related to code quality from the analysis results.
- Ability to specify the location of a custom supported JDK or JRE version that is not included in the Fortify Static Code Analyzer installation
- Fortify Static Code Analyzer automatically detects the content of files with a .cls extension to determine if they are Apex or Visual Basic code. This removes the need to include the -apex option, which is now deprecated.
- Updated LOC (lines of code) calculation: To better align with the LOC count shown by code editors, Fortify Static Code Analyzer now reports the total number of lines of code, including blank lines and comments. Due to this change, when you upload an artifact created with Fortify Static Code Analyzer 24.2.0 (or later) to an SSC application version that already contains artifacts generated by earlier versions of Fortify Static Code Analyzer, a one-time approval may be required if the following processing rule is enabled: `Require approval if line count differs by more than 10%`. Once a 24.2.0 artifact has been approved in an application version, subsequent 24.2.0 uploads to that application version will no longer trigger the processing rule unless the LOC count changes due to significant code changes or changes in the scan setup.

# Fortify Static Code Analyzer Tools

The following features have been added to Fortify Static Code Analyzer tools.

**Fortify Applications and Tools Installer**

Now includes the standalone Fortify ScanCentral SAST client.

**Fortify Audit Workbench**

Now includes a timeout setting for downloading analysis results from Fortify Software Security Center.

**Secure Coding Plugins**

- Support for Red Hat Enterprise Linux (RHEL) 9
- Support for macOS 14
- Fortify Visual Studio Extension supports suppressing issues and auditing multiple issues in batch when remediating analysis results on Fortify Software Security Center.
- Fortify Plugin for Eclipse, Fortify Analysis Plugin for IntelliJ IDEA and Android Studio, and the Fortify Extension for Visual Studio support analysis with a standalone ScanCentral SAST client.
- Support for Eclipse 2023-12 and 2024-03
- Support for IntelliJ IDEA 2023.3 and 2024.1
- Support for Android Studio 2023.1 and 2023.2
- The Fortify Analysis Plugin for IntelliJ IDEA and Android Studio, Fortify Plugin for Eclipse, and Fortify Extension for Visual Studio will be available in the relevant marketplaces.

**New Issue Reports**

- DISA STIG 5.3
- OWASP Mobile Top 10 2024

# Fortify ScanCentral DAST

The following features have been added to ScanCentral DAST.

**Syncing of Suppressed Issues in Fortify Software Security Center**

You can now configure Kafka settings in ScanCentral DAST to provide support for the syncing of audit history changes in Fortify Software Security Center, including support for suppressed issues. Additionally, you can show or hide suppressed issues in the ScanCentral DAST Scans view and scan visualization.

**Regex Editor Tool**

ScanCentral DAST now includes a Regex Editor tool that enables you to construct and test regular expressions.

**Perform Actions on Multiple Scans**

You can select multiple scans and then pause, start, stop, delete, or publish them.

**Use an Access Token for Sensor Auto Scaling**

When configuring Sensor Auto Scaling in a Kubernetes environment, you can now configure ScanCentral DAST to read an access token from the default path in Kubernetes, to retrieve the token from a specific path in the container, or to use a long-lived access token.

**DAST Health Monitoring**

Readiness and liveness probe commands have been added to ScanCentral DAST services to enable Kubernetes to detect failures and restart containers.

**OAuth 2.0 Support**

You can now configure Client Credentials Grant and Password Credentials Grant OAuth 2.0 authentication flows for scans requiring network authentication.

**Mac Version of Event-based Web Macro Recorder Tool**

The Event-based Web Macro Recorder tool is available for Mac, which enables you to create login and workflow macros on macOS.

## Fortify WebInspect

The following features have been added to WebInspect.

**Docker Images Available in Iron Bank**

The Fortify WebInspect (DAST) scanner Docker image is available on the Iron Bank hardened container image repository, along with the 2FA, FAST, OAST, and WISE images.

**Enhanced CycloneDX Export Data**

CycloneDX export data now includes vulnerability details, including CVE ID number, description, ratings, affected library versions, and the source provider's URL (PURL).

**OAuth 2.0 Support**

You can now configure Client Credentials Grant and Password Credentials Grant OAuth 2.0 authentication flows for scans requiring network authentication.

**Mac Version of Event-based Web Macro Recorder Tool**

The Event-based Web Macro Recorder tool is available for Mac, which enables you to create login and workflow macros on macOS.

# What's New in Fortify Software 23.2.0

## December 2023

This release of Fortify Software includes the following new functions and features.

## Fortify Software Security Center

The following features have been added to Fortify Software Security Center.

**Fortify Audit Assistant Gen 2**

Audit Assistant is an optional tool that you can use to help determine whether or not the issues returned from your scans represent true vulnerabilities. Generation 2, or Gen 2, of Audit assistant is now available. Using advanced AI and machine learning, Gen 2 provides improved accuracy, training based on the decisions your auditors have made, and greater speed.

When upgrading Application Security Software to version 23.2.0, you must also upgrade Audit Assistant to use the new Gen 2 version of Audit Assistant.

**BIGINT Data Type Replaces INT in scan_issue(ID) and issue(ID) Fields**

This change affects the scan_issue table in both MSSQL and MySQL databases. During database migration, the data type for scan_issue(ID) and issue(ID) will be changed to BIGINT if it has not already been done. For information on how this impacts your database migration, see "Preparing to Upgrade the Fortify Software Security Center Database" in the *OpenText™ Fortify Software Security Center User Guide*.

### Debricked SBOM Support

You can now download Debricked Software Bill Of Materials and view information on the third-party components in your application.

### Base URL Attribute

You can now assign a base URL attribute via the SCANCENTRAL DAST ATTRIBUTES page.

### New Automation Token

Fortify Software Security Center now has a new SSC API Token type: the AutomationToken. This token type is a duplicate of the UnifiedLoginToken type. It provides access to most of the REST API and is intended for use in long-running automations and can be configured to last up to a year.

### Preserve Issue Detected on Date Across Versions

Now, when creating a new application version based on a previous version, the **Detected on** date will be carried over to the new version. Previously, the **Detected on** date was set to the current date when basing a new application version on a previous one.

### Change User Assigned to an Issue

You can now change the user assigned to an issue.

### Custom Banner

An administrator can create an informational banner that persists until removed or changed.

### New Reports

The premium report bundle now includes two new issue reports:

- OWASP API Top 10 (2023)
- CWE Top 25 (2023)

The following report versions are no longer available in this release:

- SANS 2009/2010
- STIG 4.10, 4.9 and below
- OWASP < 2013
- CWE Top 25 2019/2020
- WASC 24 + 2

### REST Fortify Client

The REST fortifyclient replaces the SOAP fortifyclient and is now the default.

### Additions to the System Requirements

Fortify Software Security Center Database

- SQL Server 2022

### Service Integrations

- Jira 9.10

### Software Requirements

- Red Hat Enterprise Linux 9 (RHEL 9) support
- Kubernetes 1.27 and 1.28 support
- Helm 3.12 support

### BIRT Reporting

- BIRT Report Designer 4.13.0

# Fortify ScanCentral SAST

The following features have been added to Fortify ScanCentral SAST.

- Support for ScanCentral SAST .NET scanning and packaging on Linux systems
- Support for remote translation and scan of COBOL projects
- ScanCentral SAST will now retry any failed uploads to Fortify Software Security Center. Use the new upload command to resend an FPR file to Fortify Software Security Center after a previous upload attempt failed.
- REST API documentation for the Fortify ScanCentral SAST Controller is available with Swagger UI
- You can now package the debug logs from clients, sensors, and Fortify Static Code Analyzer into a ZIP archive using the start command option `-diagnosis`.
- Offload translation and scan support with Gradle versions 7.4-8.3 and MSBuild versions 17.4 - 17.8

# Fortify Static Code Analyzer

The following features have been added to Fortify Static Code Analyzer:

**Build tools**

- Ant 1.10.14
- Gradle 8.1 and 8.3
- Maven 3.9.4
- MSBuild 17.6 - 17.8
- xcodebuild 15 and 15.0.1

**Languages**

- Angular 15.1, 15.2, 16.0
- Apex 58
- Bicep v0.12.x → current
  - 0.12.1 → 0.14.85 (supporting .NET 6)
  - 0.15.31 → current (supporting .NET 7)
- C# 12
- C17
- Dart 3.0
- ECMAScript 2023
- Go 1.20
- Kotlin 1.8
- .NET 8.0
- Python 3.12
  - Django up to 4.2
- React 18.0
- Solidity 0.4.12-0.8.21
- Swift 5.9
- TypeScript 5.0

**Compilers**

- Clang 15.0.0
- Swiftc 5.9

# Fortify Static Code Analyzer Tools

The following features have been added to Fortify Static Code Analyzer tools.

The Fortify Static Code Analyzer installer no longer includes the Fortify Static Code Analyzer applications and tools. A separate installer is included for installing the Fortify Static Code Analyzer applications and tools.

**Fortify Audit Workbench**

- Syntax source code highlighting for Terraform, Dart, Bicep, and Solidity.
- Installation automatically detects the Fortify Static Code Analyzer versions installed in a default location.
- By default, Fortify Audit Workbench does not display binary source code

**Secure Coding Plugins**

- Fortify Plugin for Eclipse adds support for 2023-06 and 2023.06
- Fortify Analysis Plugin for IntelliJ IDEA and Android Studio adds support for IntelliJ IDEA 2023.2 and Android Studio 2022.2 and 2022.3

**New Report Versions**

OWASP MASVS 2.0

CWE Top 25 2023

OWASP API Top 10 2023

# Fortify ScanCentral DAST

The following features have been added to ScanCentral DAST

**Fortify Connect**

The new Fortify Connect feature enables you to perform scans of private applications from the cloud without exposing the application through your firewall.

**Event-based Logout Conditions**

The Event-based Web Macro Recorder now supports the use of JavaScript during execution to detect and notify the Fortify WebInspect sensor of logout.

**Event Handlers**

The Event-based Web Macro Recorder now supports event handlers that react to unpredictable events, such as dialogs opening and popup DOM elements that steal focus.

**Web Storage Keys**

The Event-based Web Macro Recorder now supports the use of web storage keys that enable the application to determine and maintain state.

**Support for IMAP in Two-factor Authentication Scans**

Two-factor authentication scanning now supports IMAP email servers.

# Fortify WebInspect

The following features have been added to Fortify WebInspect.

**Fortify License and Infrastructure Manager**

Linux Version

A Linux version of the Fortify License and Infrastructure Manager (LIM) is now available for download from the Fortify Docker repository.

**Event-based Logout Conditions**

The Event-based Web Macro Recorder now supports the use of JavaScript during execution to detect and notify the Fortify WebInspect sensor of logout.

**Event Handlers**

The Event-based Web Macro Recorder now supports event handlers that react to unpredictable events, such as dialogs opening and popup DOM elements that steal focus.

**Web Storage Keys**

The Event-based Web Macro Recorder now supports the use of web storage keys that enable the application to determine and maintain state.

**Web Socket Events**

WebInspect now includes a Capture Web Socket Events setting in the JavaScript dialog under Scan Settings.

**Support for IMAP in Two-factor Authentication Scans**

Two-factor authentication scanning now supports IMAP email servers.