OpenText™ Fortify Software, Version 24.2.0

Release Notes

Document Release Date: May 2024
Software Release Date: May 2024

This document provides installation and upgrade notes, known issues, and workarounds that apply to release 24.2.0 of the Fortify product suite.

This information is not available elsewhere in the product documentation. For information on new features in this release, see *What's New in Fortify Software 24.2.0*, which is available on the Product Documentation website:

https://www.microfocus.com/support/documentation.

UPDATES TO THIS DOCUMENT

Date	Addition and/or changes
5/23/2024	Initial release.
5/24/2024	A Fortify ScanCentral DAST Configuration Tool CLI availability note was added to the Fortify ScanCentral DAST section under INSTALLATION AND UPGRADE NOTES.

FORTIFY DOCUMENTATION UPDATES

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 *Fortify WebInspect Agent Installation and Rulepack Kit Guide*.

Accessing Fortify Documentation

The Fortify Software documentation set contains installation, deployment, and user guides. In addition, you may find technical notes and release notes that describe forthcoming features, known issues, and last-minute updates. You can access the latest HTML or PDF versions of these documents from the Product Documentation website:

https://www.microfocus.com/support/documentation.

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

INSTALLATION AND UPGRADE NOTES

Complete instructions for installing Fortify Software products are provided in the documentation for each product.

Fortify ScanCentral SAST

- Java 17 is required for both the Controller and client
- If upgrading from versions 23.1.x and older, use the DB migration script to migrate the Controller's database.

SWFScan Removed

- The SWFScan tool has been removed from the Fortify WebInspect toolkit.

Fortify License and Infrastructure Manager (LIM) Docker Images

- Do not deploy a LIM Docker image in an air-gapped environment.
- If using Kubernetes, do not run the LIM container inside the cluster.

Fortify License and Infrastructure Manager (LIM) Standard Installation

When installing the 24.2.0 LIM on a Windows server and using an existing site for the LIM, you must set "Load User Profile" to true in the advanced settings for the application pool. Otherwise, the LIM will not allow login after the application restarts. If you update the value after the LIM web site has started, then you must restart the application pool.

Fortify ScanCentral DAST

The ScanCentral DAST Configuration Tool CLI is available as an executable (EXE) file and as Docker images. For customers in air-gapped environments, TAR files are available. The EXE file should have been included in the download package but was inadvertently not included in the 24.2.0 download package. Contact Customer Support for the EXE file or the TAR files.

USAGE NOTES FOR THIS RELEASE

There is a landing page (https://fortify.github.io/) for our consolidated (Fortify on Demand + Fortify On-Premises) GitHub repository. It contains links to engineering documentation and the code to several projects, including a parser sample, our plugin framework, and our JavaScript Sandbox Project.

Fortify Static Code Analyzer

- To translate Python Django Framework code, you must include the –`Dcom.fortify.sca.PythonV2=false` option.
- Updated LOC (lines of code) calculation: The LOC calculation returns the total number of new lines, including blank lines and comments. The LOC value is closely aligned with what you might see in your code editor. Because of changes to how LOC is calculated, these values should not be compared to values achieved with previous releases of OpenText Fortify Static Code Analyzer.

Fortify ScanCentral SAST

- ScanCentral SAST client now accepts an encoded Software Security Center authentication token for the `-ssctoken` and `-uptoken` options. Support for the decoded token is deprecated and will be removed in a future release.

Fortify Software Security Center

- Flexible job execution strategy replaces Conservative job execution strategy as the default strategy. It supersedes other execution strategies (Conservative, Aggressive, Exclusive jobs), which are now deprecated and will be removed in future release. When upgrading from a previous Fortify Software Security Center release, any configured strategy will be maintained. It is recommended to switch to the Flexible job execution strategy on existing installations.

- Significant improvements were delivered in Fortify Audit Assistant in 23.2.0 release. If you are migrating from a version of Fortify Software Security Center earlier than 23.2.0, manual migration steps are required to continue using Fortify Audit Assistant integration. For more details, see "Updating the Fortify Audit Assistant Configuration" in the *Fortify Software Security Center User Guide* after upgrading.

- The response code returned from the `api/v1/projects/{id}` endpoint in case of non-existing resource or missing user's permissions is changed from 409 (Conflict) to 403 (Forbidden) to make it consistent with other endpoints.

- The `Index New Issues` job, which runs after each artifact upload is completed to ensure data consistency, now runs as a system job without any user. Previously, this job was run under the user who uploaded the related artifact.

- LDAP cache properties adjusted to better suit production environments. Cache refresh interval has been increased to 6 hours which reduces the overhead of cache reloading. Cache persistence is now enabled by default which allows faster Fortify Software Security Center restarts (especially in large LDAP environments) by retaining the cache.

- The output of REST API based `fortifyclient's` token `-gettoken` command changed from a two-line form (Authentication token on the first line and the generated token on second line) to one-line output in the form of Authorization token: `<generated token>`. The change was done to make the output backward compatible with the former SOAP API based `fortifyclient`.

- Note the following important changes related to the SOAP API removal:
  - As previously announced, SOAP API is removed and cannot be enabled.
  - The following tokens, that only had SOAP API capability, are no longer available: `AuditToken`, `ScanCentralOneTimeJobToken`, `WIESystemToken`, and `WIEUserToken`. Already existing generated tokens of listed types are revoked and removed during database migration.

- REST API-based `fortifyclient` is the primary `fortifyclient`. It is in the `Tools/fortifyclient` folder.
- SOAP API-based `fortifyclient` is no longer available.
- The `/download/documentTemplateDownload.html` endpoint was removed without replacement.
- It is not possible to create new Application version with FULL or ASSESSMENT mode through REST API anymore. Such requests will be rejected. The mode defaults to BASIC, which is the only allowed value starting from this release. Existing Application versions are not modified.
- Requirement Templates are completely removed. It is not possible to use them to assign Issue Templates to Application Versions (which was their only remaining functionality in the previous release).
- Existing alerts with obsolete monitoredEntityType `RT_INSTANCE`, `REQ_INSTANCE` and `ACTIVITY_INSTANCE` cannot trigger and are removed by migration.
- If you use custom generated Report Templates, make sure your templates do not query any of the following tables (which are removed completely by migration): `activitycomment, activityinstance, activitysignoff, documentai, documentartifact, documentartifact_def, documentdefinstance, measurementinstance, projectstateai, requirementcomment, requirementinstance, requirementsignoff, requirementtemplatecomment, requirementtemplateinstance, requirementtemplatesignoff, savedevidence, sdlhistory, taskcomment, taskinstance, timelapse_event, timelapseai, variableinstance.`

KNOWN ISSUES

The following are known problems and limitations in Fortify Software 24.2.0. The problems are grouped according to the product area affected.

Fortify Software Security Center

- Enabling the "Enhanced Security" option for BIRT reports breaks report generation if Fortify Software Security Center is installed on a Windows system.
- For successful integration with Fortify WebInspect Enterprise, Fortify Software Security Center must be deployed to a `/ssc` context. The context must be changed for a Fortify Software Security Center Kubernetes deployment, which uses root context by default.
- The migration script downloaded from the maintenance page will be saved to 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`.

- Fortify Software Security Center does not verify optional signature on SAML identity provider metadata even if it is present. Recommended mitigation is to use `file://` or `https:// URL` to provide the identity provider's SAML metadata to Fortify Software Security Center (avoid using `http:// URL`).
- Fortify Software Security Center API Swagger spec contains two definitions that differ only in case:
  - `Custom Tag` is used for assigning custom tag values to issues in an application version.
  - `Custom tag` is used for managing custom tags.

Please pay attention when using tools to auto-generate API clients from the Swagger spec. It may cause conflicts due to its case insensitive process. The generated client might need manual modification.

Fortify Static Code Analyzer

- When using Fortify Security Content 2023 Update 1 and Fortify Static Code Analyzer 23.1.0 or later, Fortify provides a default set of strict regular expression rules that can be customized using properties defined in the `<sca_install_dir>/Core/config/fortify-rules.properties`. The new default rules are stricter than in previous releases in order to minimize false positives.
- Scans involving Bicep code must not include backslashes ('\') in any file names or directory names (for example, "`m\yFile.txt`"). Backslashes as a path separator work as intended. This is a limitation of .NET 6.0 and should be fixed in a future release. (Windows does not allow backslashes in file and directory names).
- Scanning Salesforce Apex: Our documentation guide describes using the Salesforce Ant Migration Tool to set up the project and provide the dependencies. Fortify does not officially support Visual Studio Code projects, however with a recent Visual Studio Code update you can download the stubs and sObjects into a top folder called `.sfdx`, and in subfolders `StandardApexLibrary` and `standardObjects` (the full path depends on the Apex version used). This creates problems/conflicts with the stubs shipped with Fortify Static Code Analyzer. If using Visual Studio Code, you must exclude `.sfdx` or those specific folders from the translation.

Fortify Audit Workbench, Secure Code Plugins, and Tools

- In Audit Workbench, Smart View does not work on Windows 11 / Windows Server 2022 due to the default browser on these platforms being set to Edge. Changing the default browser to Chrome resolves the 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.

Fortify ScanCentral DAST, OAST, WebInspect, and 2FA Server UBI Base Docker Image Names

Due to frequent base image updates caused by UBI security fixes, Fortify no longer includes the minor version for UBI base images for the ScanCentral DAST, OAST, WebInspect, and 2FA Server products or product components.

NOTICES OF PLANNED CHANGES

This section includes product features that will be removed from a 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. Fortify recommends that you remove deprecated features from your workflow at your earliest convenience.

Note: For a list of **technologies** that will lose support in the next release, see the "Technologies to Lose Support in the Next Release" topic in the *Fortify Software System Requirements* document.

Fortify Product Portfolio

Beginning in 2024, Fortify product GA versions will transition to be in parity with OpenText release versioning. Product versions will be based on the targeted release year and quarter. This change only impacts product versions that do not currently follow this versioning strategy.

For example:

2023 release versioning

- Fortify Static Code Analyzer 23.1.0 *(release targeted for 2nd quarter 2023)*
- Fortify Static Code Analyzer 23.2.0 *(release targeted for 4th quarter 2023)*

2024 release versioning, and beyond

- Fortify Static Code Analyzer 24.2.0 *(release targeted for 2nd quarter 2024)*
- Fortify Static Code Analyzer 24.4.0 *(release targeted for 4th quarter 2024)*

Fortify ScanCentral SAST

- In 23.1.0, the arguments command is deprecated. To set additional translation arguments, use the `–targs` option of the start or package commands. To set additional scan arguments, use the `–sargs` option of the start command.
- In 24.2.0, the use of the decoded Software Security Center authentication token for the `–ssctoken` and `–uptoken` options is deprecated. Use the encoded token instead.

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 Fortify Software Security Center. Fortify 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 Fortify Software Security Center after the migration. If you choose to continue using Bugzilla, in order to mitigate the issue, you must ensure that Fortify Software Security Center 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 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 Fortify Software Security Center.
- Kerberos/SPNEGO and CAS single sign-on solutions will be deprecated starting in the next release (24.4.0) and will be removed from Fortify Software Security Center in the 25.2.0 release.
- Oracle 12c support will be removed in the next release.
- REST API POST operation at `/api/v1/issues/{parentId}/comments` is deprecated (not visible in Swagger UI, but still functional) and will be removed in the next release. Migrate to `/api/v1/projectVersions/{parentId}/issues/action/audit`.
- Flexible job execution strategy replaces Conservative job execution strategy as the default strategy. It supersedes other execution strategies (Conservative, Aggressive, Exclusive jobs), which are now deprecated and will be removed in a future release. When upgrading from a previous Fortify Software Security Center release, any configured strategy will be maintained. Fortify recommends that you switch to the Flexible job execution strategy on existing installations.
- REST API endpoints `/api/v1/personas` (Persona management) and `/api/v1/projectVersions/{parentId}/responsibilities` (lists and assigns responsibilities through Personas to a user for a given Application Version) are deprecated (not visible in Swagger UI, but functional) and will be removed in the next release with no replacement. The persona-based functionality is no longer used in Fortify Software Security Center.
- `VSTSExtensionToken` is deprecated and will be removed in the next release. Please use `ScanCentralCtrlToken` instead.

Fortify License and Infrastructure Manager

- Starting in version 24.2.0, the Fortify License and Infrastructure Manager (LIM) is available as a Windows installed version and as a Linux container. The Windows container for the LIM has been deprecated.

Fortify ScanCentral DAST

- The DAST API v1 has been deprecated as indicated in the DAST API Swagger UI. It will be removed from the product in the 24.4.0 release.

- ScanCentral DAST 24.4.0 will include a new composite settings ZIP file that will replace the XML settings file format. ScanCentral DAST 24.4.0 will not support downloading the settings file in the XML format. Settings files downloaded from the ScanCentral DAST UI will be in the new composite settings ZIP file format. The following API endpoint will be disabled:

  ```
  /api/v<version:apiVersion>/application-version-scan-
  settings/<scanSettingsId:int>/download-scan-settings-xml
  ```

- Starting in version 25.2.0, Fortify ScanCentral DAST will be available as Linux containers only. The Windows containers for Fortify ScanCentral DAST will be deprecated.

Fortify WebInspect

- 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. We recommend 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 version 24.4.0.

Fortify Applications and Tools

- Starting in version 24.2.0, Bugzilla support is deprecated and will be removed from the product in version 24.4.0.

The SOAP API-based `fortifyclient` deprecation schedule:

Fortify Apps and Tools version 23.2.0

- The REST API-based `fortifyclient` is the primary `fortifyclient` utility. It is located in the bin folder.
- The SOAP API-based `fortifyclient` is still available in an alternate folder: `tools`.
- This is your last opportunity to report any missing or insufficient functionality in the REST version of `fortifyclient` prior to deprecation of the SOAP version in 24.2.0.

Fortify Apps and Tools version 24.2.0

- REST API-based `fortifyclient` will be the primary `fortifyclient`. It will be in the `bin` folder.
- SOAP API-based `fortifyclient` will be fully deprecated and no longer available.

- The Custom Rules Editor might be redesigned and replaced with an alternate tool in a future release of Fortify Static Code Analyzer Applications and Tools.
- We have removed support for Kerberos authentication to Software Security Center from Audit Workbench and the Eclipse Complete plugin.

FEATURES NOT SUPPORTED IN THIS RELEASE

The following features are no longer supported.

Fortify Software Security Center

- It is no longer possible to use the `universalAccess.allowInvalidParentId` property to modify the behavior of endpoints using a parent ID. For more details about this property, see the *Fortify Software Release Notes*, Version 23.1.0.
- `UnifiedLoginToken` and `AnalysisDownloadToken` cannot be used with the `/download/*.html` endpoints anymore. The capability was removed for security reasons. For download, single-use file transfer tokens must be used. Use `POST` at `/api/v1/fileTokens` endpoint to create a single-use file transfer token; the `UnifiedLoginToken` and `AnalysisDownloadToken` are authorized to use the `/api/v1/fileTokens`.
- Filtering and pagination capabilities have never worked on `/api/v1/userSession/state`. To avoid confusion and misuse, the search query parameter ('q' parameter) and pagination parameters ('start' and 'limit' parameters) are removed from the Swagger specification.
- REST API endpoint `/api/v1/projectVersions/{parentId}/issues/openSource`, which was deprecated in 23.2.0, has been removed. Migrate to `/api/v1/projectVersions/{parentId}/dependencyScanIssues`.

Fortify Static Code Analyzer

- The `-apex` and `-apex-version` options are deprecated and will be removed in a future release.
- Fortify Static Code Analyzer no longer supports Visual Studio Web Site projects. You must convert your Web Site projects to Web Application projects to ensure that Fortify Static Code Analyzer can scan them.

Note: For a list of technologies that are no longer supported in this release, see the "Technologies no Longer Supported in this Release" topic in the *Fortify Software System Requirements* document. This list only includes **features** that have lost support in this release.

DEFINITIONS

DEPRECATION

When a product feature or integration is deprecated Fortify will no longer accept Enhancement Requests for the feature but will respond to critical defects or security defects. Fortify will continue to support the usage of a deprecated feature or integration. If applicable, the feature will be turned off by default, but customers are able to re-enable it. Fortify 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 Fortify will no longer accept or respond to critical defects or security defects. If the feature is a function, coded in the product, all code will be removed, and the feature will no longer function in the product. If the feature is an external system or integration, the ability to integrate or be used by the product will be removed and Fortify will no longer support 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://www.microfocus.com/support.

LEGAL NOTICES

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.