OpenText™ Fortify Software, Version 23.2.0
Release Notes

Document Release Date: December 2023
Software Release Date: December 2023

IN THIS RELEASE

This document provides installation and upgrade notes, known issues, and workarounds that apply to release 23.2.0 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 23.2.0*, which is available on the Product Documentation website:

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

UPDATES TO THIS DOCUMENT

Date	Addition and/or changes
12/7/2023	Initial release.
12/7/2023	Added WebInspect Enterprise issue with self-signed certificates to the WebInspect Enterprise section under Known Issues.
12/13/2023	In the FORTIFY DOCUMENTATION UPDATES: Listed changes to the *System Requirements for Fortify Software* document to address changes to Xcode product support.
12/15/2023	Added a note on Java support in Fortify Static Code Analyzer to the INSTALLATION AND UPGRADE NOTES section.
12/18/2024	Added a workaround for the Fortify ScanCentral SAST database migration issue to the INSTALLATION AND UPGRADE NOTES section.
1/3/2024	Added a workaround to address Chrome and Firefox browser changes that prevent LIM self-signed certificates from working to the Fortify License and Infrastructure Manager (LIM) section under KNOWN ISSUES.
1/11/2024	Added a note in the INSTALLATION AND UPGRADE NOTES section on installing Fortify License and Infrastructure Manager (LIM) Docker Images.
2/28/2024	Added a note on the MySQL database migration value to the Fortify Software Security Center section under INSTALLATION AND UPGRADE NOTES.
3/13/2024	Added a workaround to the Fortify ScanCentral DAST section under INSTALLATION AND UPGRADE NOTES that address a timeout while updating the ScanCentral DAST database.

4/8/2024	Added a workaround to the Fortify ScanCentral DAST section under KNOWN ISSUES to address the ScanCentral client issue with the proper generation of the Python path for remote translation of Python projects.

FORTIFY DOCUMENTATION UPDATES

The *Fortify Static Code Analyzer Tools Properties Reference Guide* is no longer published. The information from this reference guide is now included in the *OpenText™ Fortify Static Code Analyzer Applications and Tools Guide*.

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*.

The Xcode requirements in the *Fortify Software System Requirements* for Fortify Static Code Analyzer should read as follows:

Build Tools

- xcodebuild: 14, 14.0.1, 14.1, 14.2, 14.3, 14.3.1, 15, 15.0.1 (Note: 13.x releases are no longer supported)

Languages

- Swift 5.9

Compilers

- Swiftc: 5.7, 5.7.1, 5.8, 5.8.1, 5.9 (Note: 5.5.2, 5.6, and 5.6.1 are no longer supported)
- Clang: 14.0.0, 14.0.3, 15.0.0 (Note: 13.0.01 and 13.1.6 are no longer supported)

To Lose Support in the Next Release

- xcodebuild: 13.2, 13.2.1, 13.3, 13.3.1, 13.4, 13.4.1
- Swiftc: 5.5.2, 5.6, 5.6.1
- Clang: 13.0.0, 13.1.6

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 Software Security Center

Preparing to Upgrade the Fortify Software Security Center Database (MySQL): In the Fortify Software Security Center User Guide, we recommend that you set the `innodb-buffer_pool_size` variable to 2.5 GB to accommodate database migration. Instead, the variable should be set to 85-90% of available memory. After the upgrade, revert to your previous setting.

Fortify Static Code Analyzer

By default, Fortify Static Code Analyzer supports LTS Java versions 1.8, 11, and 17. However, the -jdk (-source) option (and the `com.fortify.sca.JdkVersion` configuration property) available for scanning Java projects accept the following parameters for the Java version: 1.7, 1.8, 1.9, 7, 8, 9, 10, 11, 12, 13, 14, and 17. To scan a Java project that uses a non-LTS version of Java from the supported range of Java 7.0-17, you need to do the following:

1. Place a copy of the JRE library folder into the `<sca_install_dir>/Core/bootcp` folder.
2. Rename the JRE library folder with the version number of the JRE, such as 14 or 15.

Fortify ScanCentral DAST

- If a timeout occurs while updating the ScanCentral DAST database with the latest database schema, you can use the `generateMigrationScript` as a workaround. For more information, see “Generating a Migration Script” in the Fortify ScanCentral DAST Configuration and Usage Guide.

Fortify ScanCentral SAST

- ScanCentral client does not properly generate the Python path for remote translation of Python projects. This issue will be fixed in the next release. As a workaround in version 23.2.x, you must specify the path to the Lib folder for the Python installation with `-targs` option. For example:

```
scancentral -url <ctrl_url> start -bt none -pv 3 -pyr
requirements.txt -targs "-python-path
C:\username\AppData\Local\Programs\Python\Python311\Lib"
```

- If a timeout occurs while updating the ScanCentral DAST database with the latest database schema, you can use the `generateMigrationScript` as a workaround. For more information, see "Generating a Migration Script" in the Fortify ScanCentral DAST Configuration and Usage Guide.
- When configuring a sensor machine for remote translation of .NET projects, the sensor machine requires .NET Framework 4.7.2 or higher and .NET 6.0. Without .NET 6.0, the sensor might accept the .NET remote translation job, but the translation will fail.
- If you are upgrading the Fortify ScanCentral SAST Controller from a previous version, there is an issue with migrating the previous version's database. We are working on a patch release to fix this issue. Fortify recommends that you wait for the patch release if you are upgrading. If you choose not to wait for the patch, there is a workaround:
- Allow all jobs to finish and shut down the existing Controller.
- Backup your existing ScanCentral SAST Controller files.

1. Unzip the `Fortify_ScanCentral_Controller_23.2.0_x64.zip` and open the `db-migrate/migrate[.bat]` script in a text editor.
2. Locate the line that starts with:
    a. In the `migrate.bat` script (line 59): `"%JAVA_CMD%" -cp "%CTRL_PATH%\WEB-INF\lib\h2-1.4.200.jar"`
    b. In the migrate script (line 55): `${JAVA_CMD} -cp ${CTRL_PATH}/WEB-INF/lib/h2-1.4.200.jar`
3. Update the value of the h2 JAR file based on the version you are upgrading from:
    a. 23.1.0 -> h2-2.1.214.jar
    b. 22.2.x -> h2-2.1.212.jar
    c. 22.1.x -> h2-1.4.200.jar (no need to modify)
    d. 21.2.x -> h2-1.4.200.jar (no need to modify)
4. Run the `migrate[.bat]` script.
5. Copy the `cloudCtrlDb` directory generated in step 6 and the `jobFiles` directory from the existing Controller into the 23.2.0 Controller.
6. Start the 23.2.0 Controller, as soon as the Controller is up, immediately stop the Controller.
7. Create a file named `script.sql` and paste the following:

```
update job set requiredOs='0' where requiredOs='ANY';
```

8. Run the following Java command after updating the path values to your environment:

```
java -Dcatalina.base=C:\scancentral\controller_23.2.0\
tomcat -cp C:\scancentral\controller_23.2.0\tomcat\
webapps\scancentral-ctrl\WEB-INF\lib\*;C:\scancentral\
controller_23.2.0\tomcat\webapps\scancentral-ctrl\WEB-INF\
classes org.h2.tools.RunScript -url jdbc:h2:C:\scancentral\
controller_23.2.0\tomcat\cloudCtrlDb\db -script
script.sql -user sa
```

9. Start the 23.2.0 Controller.

Site Explorer Removed

The Site Explorer 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.

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.

Fortify Software Security Center

- A major upgrade of libraries providing functionality for SAML Single Sign On and Single Logout solutions was delivered in 22.2.0 release. If you are migrating from a version of Fortify Software Security Center earlier than 22.2.0, make sure to follow the SAML migration steps listed in the *Micro Focus Fortify Software Release Notes, Version 22.2.0*.
- To improve security for X509 SSO authentication, Fortify Software Security Center will reject requests without the X509 authentication certificate, even though the request includes a valid session cookie. To improve security for HTTP SSO authentication, Fortify Software Security Center will reject requests without the HTTP authentication header, even though the request includes a valid session cookie.
- During the migration process, orphaned data will be cleaned up from Fortify Software Security Center database. Data marked for cleanup are orphaned resources that were left behind due to incorrect handling of delete operations in previous releases. Although the cleanup will only remove orphaned unused data, we strongly recommend you backup your database before migration.
- The `/download/currentStateFprDownload.html` endpoint will include `externalmetadata.xml` file in the downloaded FPR if `clientVersion` parameter is not specified. Previously, the endpoint included `externalmetadata.xml` file only when the `clientVersion` parameter specified a version higher than 3.60.0000. If you wish to exclude `externalmetadata.xml` file from the downloaded FPR, you need to use the `clientVersion` parameter and specify a version lower than 3.60.0000.
- Scheduler Flexible job execution strategy has changed from a technical preview to a stable release. It is now the recommended scheduler job execution strategy for new

installations. It supersedes other execution strategies (Conservative, Aggressive, Exclusive jobs), which are now deprecated and scheduled for removal in the 24.4 release. When upgrading from a previous Fortify Software Security Center release, any configured strategy will be maintained.

- The base image for the Fortify Software Security Center docker container image was updated from Red Hat ubi8 to Red Hat ubi9-minimal.
- Fortify Software Security Center Helm chart Kubernetes deployment now restricts deployment to nodes with `Kubernetes.io/os=linux` and `Kubernetes.io/arch=amd64` labels using `nodeSelector`. The default `nodeSelector` settings can be overridden via `nodeSelector` Helm chart value.
- When copying an application version including application state, issues will now maintain their original introduced date (date the issue was detected on). Previously, their original introduced date was replaced by the date of the latest scan of the application version the issues were copied from. For more details, see the *OpenText™ Fortify Software Security Center User Guide 23.2.0*.
- Fortify Software Security Center requires OpenJDK 17 runtime. For more details, see the *Fortify Software System Requirements* document.
- Significant improvements were implemented in Fortify Audit Assistant. To continue using Fortify Audit Assistant integration, manual migration steps are required. For more details, see "Updating the Fortify Audit Assistant Configuration" in the *Fortify Software Security Center User Guide version 23.2.0* after upgrading.
- During migration, the `scan_issue` table type of id column will be changed from INT to BIGINT on MySQL and SQL Server databases to avoid reaching the maximum 32b integer limit.

  Any user who already applied the recommended workaround for SQL Server - reset the identity value on the *scan_issue* table to a negative number with `DBCC CHECKIDENT (scan_issue, reseed, -2147483648)` - must perform an additional manual migration step: reset the identity value back to a positive number after the migration to 23.2.0. The reset is achieved by running query: `DBCC CHECKIDENT (scan_issue, RESEED)`. The user running the query must be either an owner of the schema that contains the table, or must have `sysadmin`, `db_owner`, or `db_ddladmin` fixed database role.

- Oracle Java 17 disabled 3DES and RC4 encryption algorithms in Kerberos by default (for more details, see https://www.java.com/en/configure_crypto.html#Disable3DESandRC4). This change was also followed by various OpenJDK distributions. Fortify strongly recommends that you test Kerberos SSO behavior after the upgrade in a non-production environment first. If any of the disabled encryption algorithms are used in communication between your KDC and clients, Kerberos SSO login will fail and `ssc.log` will include a WARN with message "Negotiate Header was invalid" followed by cause (example for RC4: "Encryption type RC4 with HMAC is not supported/enabled"). Make sure to configure your Kerberos environment to use stronger encryption algorithms. As a temporary workaround, the `allow_weak_crypto` setting in the `krb5.conf` file can be used to enable 3DES and RC4. Fortify recommends you remove this setting immediately after your Kerberos environment is adjusted.
- Note the following important changes related to the scheduled SOAP API removal:

    - SOAP API is disabled by default and all SOAP API requests are rejected with a "410 Gone" response.
    - If necessary, SOAP API can be re-enabled by setting the `soap.api.disabled` property in `app.properties` to `false`. Fortify strongly recommends enabling SOAP API only temporarily and disabling it as soon as possible. Logging any usage of SOAP API can be activated by setting the Java system property `ssc.log.soap.level=info`. SOAP API requests are logged to a separate `ssc_soap.log`. The log file is created on demand.
    - The REST API-based fortifyclient is the primary fortifyclient utility. It is in the `Tools/fortifyclient` folder. For more details about REST API `fortifyclient`, see the *Fortify Software*, *Version 23.1.0 Release Notes*.
    - REST API based `fortifyclient` is also available as a sample in the `Samples` folder.
    - The legacy SOAP API-based `fortifyclient` is still available. It is in the `Tools/fortifyclient-legacy-soap` folder.
    - The SOAP API-based samples `ProjectProvisioning` and `PackageFinder` were removed and are no longer distributed in the Samples folder.

KNOWN ISSUES

The following are known problems and limitations in Fortify Software 23.2.0. 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.

- Login to Jira Software Cloud bug tracker will appear successful even if incorrect credentials are used. The bug submission is not possible because the list of Projects is empty. To enter correct bug tracker credentials, the user must log out from Software Security Center and log in again. Note that the Jira Software Cloud does not accept a user password, only an API token. The API token can be generated in your Atlassian account (for more details, see https://support.atlassian.com/atlassian-account/docs/manage-api-tokens-for-your-atlassian-account/#Create-an-API-token).

Fortify ScanCentral SAST

- ScanCentral client does not properly generate the Python path for remote translation of Python projects. This issue will be fixed in the next release. As a workaround in version 23.2.x, you must specify the path to the Lib folder for the Python installation with `-targs` option. For example:
  ```
  scancentral -url <ctrl_url> start -bt none -pv 3 -pyr requirements.txt -targs "-python-path C:\username\AppData\Local\Programs\Python\Python311\Lib"
  ```
- When using Fortify ScanCentral SAST with gradle versions 7.x, it is possible to split functionality across multiple subprojects so that the root project doesn't have a `build.gradle` or `build.gradle.kts` file. For these projects, you must include the build tool name (`-bt gradle`) with the start and package commands.
- The `-diag (--diagnosis)` option of the Fortify ScanCentral SAST client will output an error message, "Path component should be '/'", but the zip file will still be generated. The generated zip will not include the metadata file.

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.

Fortify Audit Workbench, Secure Code Plugins, and Tools

- We have temporarily removed support for Kerberos authentication to Software Security Center from Audit Workbench and the Eclipse Complete plugin. It will be restored in the next release.
- We are removing support for NTLM proxy authentication from Audit Workbench and Eclipse Complete plugin for Software Security Center connections (not external Rulepack updates).
- If you encounter crashes with Audit Workbench on an older version of Linux, make sure you have the required GTK library version 3.22 or later.

- 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.

Fortify ScanCentral DAST Key Stores and Artifacts Repositories

Settings for Key Stores and Artifacts Repositories are currently global settings. The permissions required to edit these settings also grant users the ability to view and edit all Key Stores and Artifacts Repositories. Users should be cautious when editing settings in Key Stores and Artifacts Repositories.

Fortify WebInspect and Tools Help Files

The help included in the Fortify WebInspect and WebInspect tools installation packages has a Release Date of November 2023. However, the software was not released until December 2023.

Fortify WebInspect Enterprise and Tools Help Files

- Recent updates to Chrome and Firefox browsers prevent WebInspect Enterprise self-signed certificates from working. The WebConsole Login page does not load. In Chrome, error code `ERR_SSL_KEY_USAGE_INCOMPATIBLE` appears. The workaround for this issue is available at https://www.frameflow.com/blog/solving-chrome-err-ssl-key-usage-incompatible/.
- The help included in the Fortify WebInspect Enterprise and WebInspect tools installation packages has a Release Date of November 2023. However, the software was not released until December 2023.

Fortify License and Infrastructure Manager (LIM)

- Recent updates to Chrome and Firefox browsers prevent LIM self-signed certificates from working. The LIM Admin Login page does not load. In Chrome, error code ERR_SSL_KEY_USAGE_INCOMPATIBLE appears. The workaround for this issue is available at https://www.frameflow.com/blog/solving-chrome-err-ssl-key-usage-incompatible/.

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 Software Security Center

- Starting in the next release (24.2.0), Oracle 12c support will be deprecated. Oracle 12c will be completely removed in the 24.4.0 release.

The SOAP API has been disabled and is scheduled for removal.

Important changes in Fortify Software Security Center version 23.2.0

- SOAP API is disabled by default and all SOAP API requests are rejected with a "410 Gone" response. Use REST API (`/api/v1/*, /download/*`, and co `/transfer/*`) endpoints instead of SOAP API (`/fm-ws/*`) endpoints.
- If necessary, SOAP API can be re-enabled by setting the `soap.api.disabled` property in `app.properties` to false. We strongly recommend enabling SOAP API only temporarily and disabling it again as soon as possible. Logging any usage of SOAP API can be activated by setting a java system property `ssc.log.soap.level=info`. SOAP API requests are logged to a separate `ssc_soap.log`. The log file is created on demand.
- The REST API-based `fortifyclient` is the primary `fortifyclient` utility. It is in the `Tools/fortifyclient` folder. For more details about REST API `fortifyclient`, see the *Fortify Software Release Notes*, `Version 23.1.0`.

- The REST API-based `fortifyclient` is also available as a sample in the Samples folder.
- The legacy SOAP API-based `fortifyclient` is still available. It is in an alternate folder: `Tools/fortifyclient-legacy-soap/`
- The SOAP API-based samples `ProjectProvisioning` and `PackageFinder` were removed and are no longer distributed in the Samples folder.

SOAP API deprecation schedule:

Fortify Software Security Center version 23.2.0

- SOAP API is disabled by default.
- Integration with older versions of Fortify Static Code Analyzer Applications (before version 23.2.0 for Audit Workbench, Scan Wizard, Eclipse Complete, and IntelliJ Analysis; before 23.1.0 for Eclipse/IntelliJ Remediation; before 22.1.0 for Visual Studio extension) is not supported unless SOAP API is explicitly enabled.

Fortify Software Security Center version 24.2.0

- SOAP API is removed and cannot be enabled.
- Integration with older versions of Fortify Static Code Analyzer Applications (before version 23.2.0 for Audit Workbench, Scan Wizard, Eclipse Complete and IntelliJ Analysis; before 23.1.0 for Eclipse/IntelliJ Remediation; before 22.1.0 for Visual Studio extension) is not supported.

The SOAP API based fortifyclient deprecation schedule:

Fortify Software Security Center version 23.2.0

- The REST API-based `fortifyclient` is the primary `fortifyclient` utility. It is located in `Tools/fortifyclient` folder.
- SOAP API-based `fortifyclient` is still available. It is located in an alternate folder: `Tools/fortifyclient-legacy-soap`.
- Last opportunity to report any missing or insufficient functionality in the REST version of `fortifyclient` prior to deprecation of SOAP version in 24.2.0.

Fortify Software Security Center version 24.2.0

- REST API-based fortifyclient will be the primary `fortifyclient`. It will be in the `Tools/fortifyclient` folder.

- SOAP API-based `fortifyclient` will be fully deprecated and no longer available.

Other planned changes:

- Starting from next release, it will no longer be possible to use property `permission.universalAccess.allowInvalidParentId` 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`.

- The capability to download directly (use `/download/*` endpoints directly) will be removed from `UnifiedLoginToken` and `AnalysisDownloadToken` tokens in next release 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` endpoint.
- Filtering capability was not supported on the `/api/v1/coreRulepacks` endpoint, and if the search query parameter ('q' parameter) was used, it had no effect on returned results. Therefore, the search query parameter was removed from `/api/v1/coreRulepacks` endpoint. Calling the endpoint with the search parameter will not fail the request, the parameter will be ignored.
- Filtering and pagination capability have never been supported on `/api/v1/userSession/state` endpoint. To avoid confusion and misuse, the search query parameter ('q' parameter) and pagination parameters ('start' and 'limit' parameters) will be removed from the endpoint in the next release.
- REST API endpoint `/api/v1/issues/{parentId}/comments` is deprecated and is scheduled for removal in 24.4.0 release. Migrate to `/api/v1/projectVersions/{parentId}/issues/action/audit`.
- REST API endpoint `/api/v1/projectVersions/{parentId}/issues/openSource` is deprecated and is scheduled for removal in 24.2.0 release. Migrate to `/api/v1/projectVersions/{parentId}/dependencyScanIssues`.

Fortify License and Infrastructure Manager

- Starting in version 24.2.0, the Fortify License and Infrastructure Manager (LIM) will be available as a Windows installed version and as a Linux container. The Windows container for the LIM will be deprecated. You may continue to use the existing Windows container while you consider migration options.

Fortify ScanCentral DAST

- 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.

Fortify WebInspect Enterprise

- Fortify WebInspect Enterprise 23.2.0 is the last version of the product to be released. We recommend that customers move to Fortify ScanCentral DAST for their 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 ScanCentral SAST

- The arguments command is deprecated. Use the start or package command with either the `-targs` or `-sargs` option.

Fortify Applications and Tools

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.
- Last opportunity to report any missing or insufficient functionality in the REST version of `fortifyclient` prior to deprecation of 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

- 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.

FEATURES NOT SUPPORTED IN THIS RELEASE

The following features are no longer supported.

- The following reports and their mappings have been removed by default in Fortify Software Security Center 23.2.0:
  - DISA STIG versions 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10
  - SANS Top 25 versions 2009, 2010
  - OWASP Top 10 versions 2004, 2007, 2010
  - CWE Top 25 versions 2019, 2020
  - WASC version 24 + 2

The removal of these mappings means the associated attributes associated are no longer displayed in the Group By and Filter By lists on the Audit page of Fortify Software Security Center 23.2.0.

- As previously announced, Fortify Software Security Center REST API endpoint `api/v1/projectVersions/{parentId}/dynamicScanRequests/action/cancel` was removed in this 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.

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