# OpenText™ Application Security Tools

## Tools Guide

Version : 25.4.0

PDF Generated on : 28/10/2025

# Table of Contents

# 1. Tools Guide

Software Version: 25.4.0

Document Release Date: 25.4.0

Software Release Date: 25.4.0

# 1.1. Change log

The following table lists changes made to this helpdocument. Revisions to this helpdocument are published between software releases only if the changes made affect product functionality.

| **Software Release / Document Version** | **Changes** |
|---|---|
| 25.4.0 | Added:<br>• A section for upgrading the Fortify Scan Wizard in macOS ARM64 installers (see Upgrading the Fortify Scan Wizard)<br>• Support for DISA STIG 6.2, DISA STIG 6.3, and OWASP ASVS 5.0 (see BIRTReportGenerator Command-Line Options)<br>• Added Supported file extensions for languages<br>• Added Supported file extensions in builds tools<br>• Option to list issues with additional metadata from an FPR file (see Displaying Analysis Results Information from an FPR File)<br>Removed:<br>• Removed support for `OWASP Top 10 - 2013`, `CWE Top 25 - 2021, 2022`, `STIG - 4.11, 5.1, 5.2` from the BIRT report templates (see BIRTReportGenerator Command-Line Options) |
| 25.2.0 | Updated:<br>• Incorporated product name changes (see Product name changes)<br>• The installer file name and format has changed (see Installing OpenText Application Security Tools and Installing OpenText™ Application Security Tools Silently (Unattended))<br>• The uninstaller file name and format has changed (see Uninstalling OpenText™ Application Security Tools, Uninstalling OpenText™ Application Security Tools Silently, and Uninstalling OpenText™ Application Security Tools in Text-Based Mode on Non-Windows Platforms)<br>• The location for the installer log file has changed (see Installing OpenText™ Application Security Tools Silently (Unattended))<br>• Installer for Linux and macOS on ARM-based systems (see Installing OpenText Application Security Tools) |
| 24.4.0 | Updated:<br>• Removed mention of Fortify Security Assistant Plugin for Eclipse from About OpenText Application Security Tools. This application is available in the Eclipse marketplace and has been removed from the OpenText™ Application Security Tools download package |
| 24.2.0 | Updated:<br>• Added ability to install the ScanCentral SAST client as a component of the Tools Guide installer (see About OpenText Application Security Tools, Installing OpenText™ Application Security Tools Silently (Unattended)), and Locating Log Files)<br>• Added options for updated issue report versions (see BIRTReportGenerator Command-Line Options)<br>• Description for the FPRUtility `-loc` option (see Displaying Analysis Results Information from an FPR File)<br>Removed:<br>• The `com.fortify.model.PersistenceStrategy` property from the `fortify.properties` file was removed because it has only one valid value |

# 1.2. Getting Started

This section describes the OpenText™ Static Application Security Testing applications and tools and how to install them.

This section contains the following topics:

# 1.2.1. Product name changes

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

| Previous name | New name |
|---|---|
| Fortify Static Code Analyzer | OpenText™ Static Application Security Testing (OpenText SAST) |
| Fortify Software Security Center | OpenText™ Application Security |
| Fortify WebInspect | OpenText™ Dynamic Application Security Testing (OpenText DAST) |
| Fortify on Demand | OpenText™ Core Application Security |
| Debricked | OpenText™ Core Software Composition Analysis (OpenText Core SCA) |
| 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.

# 1.2.2. About OpenText Application Security Tools

The OpenText™ Application Security Tools installation includes applications and Secure Code Plugins that enable you to scan your code with OpenText SAST and view the analysis results so you can fix vulnerability issues. The command-line tools enable you to generate reports based on the analysis results, work with Fortify Project Results (FPR) files, and securely transfer objects to and from OpenText™ Application Security.

The following table describes the OpenText SAST applications and tools that you can install with the OpenText™ Application Security Tools installer.

| Application or Tool | Description | More Information |
|---|---|---|
| OpenText™ Fortify Audit Workbench | Provides a graphical user interface for OpenText SAST analysis results that helps you organize, investigate, and prioritize analysis results so that developers can fix security flaws quickly. | *OpenText™ Fortify Audit Workbench User Guide* in Fortify Static Code Analyzer and Tools Documentation |
| OpenText™ Fortify Plugin for Eclipse | Adds the ability to run OpenText SAST scans (either locally or remotely using OpenText™ ScanCentral SAST) on the entire Java codebase of a project from the Eclipse IDE. The analysis results are displayed, along with descriptions of each of the security issues and suggestions for their elimination. | *OpenText™ Fortify Plugin for Eclipse User Guide* in Fortify Static Code Analyzer and Tools Documentation |
| OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studio | Adds the ability to run OpenText SAST scans (either locally or remotely using ScanCentral SAST) on the entire codebase of a project from IntelliJ IDEA and Android Studio. To view the analysis results, upload them to Application Security or open them in Fortify Audit Workbench. | *OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studio User Guide* in Fortify Static Code Analyzer and Tools Documentation |
| OpenText™ Fortify Extension for Visual Studio | Adds the ability to run OpenText SAST scan (either locally or remotely using ScanCentral SAST) on solutions and projects from Visual Studio. The analysis results are displayed, along with descriptions of each of the security issues and suggestions for their elimination. This extension also includes remediation functionality that works with analysis results stored on a Application Security server. | *OpenText™ Fortify Extension for Visual Studio User Guide* in Fortify Static Code Analyzer and Tools Documentation |
| OpenText™ ScanCentral SAST client | Enables you to offload OpenText SAST analysis to ScanCentral SAST, which can perform remote translation and scan of your applications. Users of Application Security can direct ScanCentral SAST to upload the analysis results to the server. | *OpenText™ ScanCentral SAST Installation, Configuration, and Usage Guide* in Fortify Software Security Center Documentation |
| Fortify Scan Wizard | Provides a graphical user interface that enables you to prepare a script to scan your code with OpenText SAST (either locally or remotely using ScanCentral SAST) and then optionally upload the results to Application Security. | Fortify Scan Wizard |
| Fortify Custom Rules Editor | Provides a graphical user interface to create and edit custom rules. | Not applicable |
| BIRTReportGenerator ReportGenerator | Command-line tools to generate BIRT reports and legacy reports based on a Fortify Project Results (FPR) file. | Generating Analysis Reports from the Command Line |

| | | |
|---|---|---|
| FPRUtility | Command-line tool that enables you to:<br>• Merge audited projects<br>• Verify FPR signatures<br>• Display information from an FPR file including:<br>  ◦ Any errors associated with the analysis<br>  ◦ Number of issues<br>  ◦ Filtered lists of issues in different formats<br>  ◦ Lines of code for analyzed files<br>  ◦ List of analyzed functions<br>  ◦ Mappings for a migrated project<br>• Combine or split source code files and audit projects into FPR files<br>• Alter an FPR | Working with FPR Files from the Command Line |
| fortifyclient | Command-line utility to create Application Security authentication tokens and securely transfer objects to and from Application Security. | *OpenText™ Application Security User Guide* in Application Security Documentation |

# 1.2.3. System requirements

This section describes the system requirements for OpenText Application Security Tools.

This section describes the system requirements for OpenText Application Security Tools and contains the following topics:

# 1.2.3.1. Hardware requirements

OpenText Application Security Tools require a system with at least 8 GB of RAM. In addition, OpenText Application Security Tools used to perform code analysis have the same hardware requirements as OpenText SAST (see Hardware Requirements).

# 1.2.3.2. Platforms and architectures

OpenText Application Security Tools support the platforms and architectures listed in the following table.

| Operating system | Platforms | Distributions and versions |
|---|---|---|
| Microsoft Windows® | x64 | 10, 11 |
| Linux® | x64<br>ARM | Red Hat Enterprise Linux 8, 9<br>SUSE Linux Enterprise Server 15<br><br>**Important**<br>Fortify Audit Workbench, Fortify Custom Rules Editor, and Fortify Scan Wizard require GTK version 3.22 or later. Some platform versions include this requirement such as Red Hat Enterprise Linux 7.4 and later. |
| macOS® | x64<br>ARM | 13, 14, 15 |

# 1.2.3.3. Software requirements

The OpenText Application Security Tools installation includes an embedded OpenJDK/JRE version 17, which the applications and tools require. You do not need to install Java 17.

To use OpenText Application Security Tools, you must have Read and Write permissions for the OpenText Application Security Tools installation directory.

To run Fortify Audit Workbench, Fortify Custom Rules Editor, or Fortify Scan Wizard remotely from a local server, you must use a remote desktop connection such as Virtual Network Computing (VNC) or Windows Remote Desktop Connection. Do not use X Window System (X11) forwarding to access these applications from a remote server.

# 1.2.3.4. Service integrations for OpenText Application Security Tools

The following table lists the supported service integrations for Fortify Audit Workbench and the Secure Code Plugins.

| Service | Versions | Supported applications |
|---|---|---|
| OpenText Application Quality Management | 12.50 | Fortify Audit Workbench<br>Fortify Plugin for Eclipse |
| Azure DevOps Server | 2019<br>2020<br>2022 | Fortify Audit Workbench<br>Fortify Plugin for Eclipse<br>Fortify Extension for Visual Studio |
| Azure DevOps<br><br>**Note**<br>Only basic user password authentication is supported. | Not applicable | Fortify Audit Workbench<br>Fortify Plugin for Eclipse |
| Jira Software Server | 8.13<br>9.10 | Fortify Audit Workbench<br>Fortify Plugin for Eclipse |
| Jira Software Cloud | Not applicable | Fortify Audit Workbench<br>Fortify Plugin for Eclipse |
| Application Security Bug Tracker | 25.4.0 | Fortify Audit Workbench<br>Fortify Plugin for Eclipse<br>Fortify Extension for Visual Studio |

# 1.2.3.5. Secure Code Plugins

The following table lists the supported integrated development environments (IDE) for the Secure Code Plugins.

| Secure Code Plugin | IDE | Versions | Notes |
|---|---|---|---|
| Fortify Plugin for Eclipse | Eclipse | 2023-x<br>2024-03<br>2024-06 | |
| Fortify Analysis Plugin for IntelliJ IDEA and Android Studio | IntelliJ IDEA | 2023.x<br>2024.1<br>2024.2 | IntelliJ IDEA Ultimate and Community Edition are supported. |
| | Android Studio | 2023.x<br>2024.1 | |
| Fortify Extension for Visual Studio | Visual Studio | 2017<br>2019<br>2022 | Visual Studio Community, Professional, and Enterprise editions for Windows are supported. For supported MSBuild versions, see Build Tools. |

# 1.2.3.6. Authentication for connecting to Application Security

In addition to user name and password authentication, Fortify Audit Workbench and all the Secure Code Plugins can use token-based and SSO authentication with Application Security.

The following table lists the SSO methods that are supported for OpenText SAST applications to connect to Application Security.

| **Application** | **SSO method** |
|---|---|
| Fortify Audit Workbench | X.509 |
| Fortify Plugin for Eclipse | X.509 |
| Fortify Extension for Visual Studio | X.509 |

# 1.2.3.7. BIRT reports

To generate BIRT reports on a Linux system from the Secure Code Plugins or the BIRTReportGenerator utility, you must install the fontconfig library, DejaVu Sans fonts, and DejaVu Serif fonts on the server.

To run the BIRTReportGenerator utility in a Linux Docker container, you must have the X Window System (X11) libraries installed in the image. The X11 libraries provide the graphical user interface API that BIRT requires for data visualization.

Example for Red Hat Enterprise Linux and CentOS:

```
yum -y install xorg-x11-xauth xorg-x11-fonts-* xorg-x11-utils
```

Example for Ubuntu:

```
apt-get install x11-apps
```

# 1.2.4. About Installing OpenText Application Security Tools

See the System requirements to make sure that your system meets the minimum requirements for each software component you plan to install. For a description of the applications and tools that you can install, see About OpenText™ Application Security Tools. You must provide a Fortify license file for the OpenText Application Security Tools installation.

OpenText recommends that you install OpenText SAST before installing OpenText™ Application Security Tools. The OpenText™ Application Security Tools installer can detect an existing OpenText SAST that is locally installed in the default location or in the same root folder where you plan to install OpenText™ Application Security Tools. If the installer successfully detects the location, the applications that require the location of OpenText SAST (Fortify Audit Workbench and the Fortify Extension for Visual Studio) will have the location automatically configured.

The following table lists the different methods of installation.

| **Installation Method** | **Instructions** |
|---|---|
| Perform the installation using a standard install wizard | Installing OpenText™ Application Security Tools |
| Perform the installation silently (unattended) | Installing OpenText™ Application Security Tools Silently (Unattended) |
| Perform a text-based installation on non-Windows systems | Installing OpenText™ Application Security Tools in Text-Based Mode on Non-Windows Platforms |

# 1.2.4.1. Installing OpenText Application Security Tools

To install OpenText SAST applications and tools:

1. Run the installer file for your operating system to start the OpenText™ Application Security Tools Setup wizard:

   - Windows: `OpenText_Application_Security_Tools_windows-x64_<version>.exe`
   - Linux: `OpenText_Application_Security_Tools_linux-x64_<version>.run` or `OpenText_Application_Security_Tools_linux-arm64_<version>.run`
   - macOS: `OpenText_Application_Security_Tools_osx-x64_<version>.app.zip` or `OpenText_Application_Security_Tools_osx-arm64_<version>.app.zip`

     Uncompress the ZIP file before you run the APP installer file.

   where *<version>* is the software release version, and then click **Next**.

2. Review and accept the license agreement, and then click **Next**.
3. Choose where to install OpenText™ Application Security Tools, and then click **Next**.

   **Important**

   Do not install OpenText™ Application Security Tools in the same directory where OpenText SAST is installed.

4. (Optional) Select the components to install, and then click **Next**.
5. Specify the path to the `fortify.license` file, and then click **Next**.
6. Specify if you want to migrate from a previous installation on your system.

   Migrating from a previous installation preserves OpenText™ Application Security Tools artifact files. For more information, see About Upgrading OpenText™ Application Security Tools.

   To migrate artifacts from a previous installation:

   1. In the Applications and Tools Migration page, select **Yes**, and then click **Next**.
   2. Specify the location of the existing installation on your system, and then click **Next**.

   To skip migration of artifacts from a previous release, leave the Applications and Tools Migration selection set to **No**, and then click **Next**.

7. If you are installing the Fortify Extension for Visual Studio, do the following:

   1. Specify whether to install the extensions for the current install user or for all users.

      The default is to install the extensions for only the current install user.

   2. Click **Next**.

8. Click **Next** on the Ready to Install page to install OpenText™ Application Security Tools and any selected components.
9. Click **Finish** to close the Setup wizard.

# 1.2.4.2. Installing OpenText™ Application Security Tools Silently (Unattended)

A silent installation enables you to complete the installation without any user prompts. To install silently, you need to create an option file to provide the necessary information to the installer. Using the silent installation, you can replicate the installation parameters on multiple machines.

**Important**

Do not install OpenText™ Application Security Tools in the same directory where OpenText SAST is installed.

To install OpenText™ Application Security Tools silently:

1. Create an options file.
    1. Create a text file that contains the following line:

        ```
        fortify_license_path=<license_file_location>
        ```

        where *<license_file_location>* is the full path to your `fortify.license` file.
    2. Add more installation instructions, as needed, to the options file.

        To obtain a list of installation options that you can add to your options file, open a command prompt, and then type the installer file name and the `--help` option. This command displays each available command-line option preceded with a double dash and the available parameters enclosed in angle brackets. For example, if you want to see the progress of the install displayed at the command line, add `unattendedmodeui=minimal` to your options file. The command-line options are case-sensitive.

        For the `enable-components` option on Windows, you can specify the `AWB_group` parameter to install Fortify Audit Workbench, Fortify Custom Rules Editor, the default bug tracker plugins, and associate FPR files with Fortify Audit Workbench. To install specific plugins, list each plugin by parameter name (the `Plugins_group` parameter does **not** install all plugins and you do not need to include it).

        The following example Windows options file specifies the location of the license file, a request to migrate from a previous release, installation of Fortify Audit Workbench (associate FPR files with Fortify Audit Workbench), Fortify Scan Wizard, Fortify Custom Rules Editor, the default bug tracker plugins, ScanCentral SAST client, Fortify Extension for Visual Studio 2022 for all users, and sets the target OpenText™ Application Security Tools installation directory:

        ```
        fortify_license_path=C:\Users\admin\Desktop\fortify.license
        MigrateTools=1
        enable-components=AWB_group,ScanCentralClient,VS2022
        VS_all_users=1
        installdir=C:\FortifyApps
        ```

        The following example is an options file for Linux and macOS that specifies the location of the license file, a request to migrate from a previous release, installation of Fortify Audit Workbench, the Fortify Plugin for Eclipse, Fortify Scan Wizard, the default bug tracker plugins, ScanCentral SAST client, and sets the target OpenText™ Application Security Tools installation directory:

```
fortify_license_path=/opt/Fortify/fortify.license
MigrateTools=1
enable-components=AWB,Eclipse,ScanWizard,ScanCentralClient
installdir=/opt/FortifyApps
```

2. Save the options file.
3. Run the silent install command for your operating system.

**Note**

You might need to run the command prompt as an administrator before you run the installer.

| | |
|---|---|
| **Windows** | `OpenText_Application_Security_Tools_windows-x64_<version>.exe --mode unattended --optionfile <full_path_to_options_file>` |
| **Linux** | `./OpenText_Application_Security_Tools_linux-x64_<version>.run --mode unattended --optionfile <full_path_to_options_file>`<br>or<br>`./OpenText_Application_Security_Tools_linux-arm64_<version>.run --mode unattended --optionfile <full_path_to_options_file>` |
| **macOS** | You must uncompress the ZIP file before you run the command.<br>`OpenText_Application_Security_Tools_osx-x64_<version>.app/Contents/MacOS/installbuilder.sh --mode unattended --optionfile <full_path_to_options_file>`<br>or<br>`OpenText_Application_Security_Tools_osx-arm64_<version>.app/Contents/MacOS/installbuilder.sh --mode unattended --optionfile <full_path_to_options_file>` |

The installer creates an installer log file when the installation is complete. This log file is in the following location depending on your operating system.

| | |
|---|---|
| **Windows** | `C:\Users\<username>\AppData\Local\Temp\OpenTextApplicationSecurityTools-<version>-install.log` |
| **Linux macOS** | `/tmp/OpenTextApplicationSecurityTools-<version>-install.log` |

# 1.2.4.3. Installing OpenText™ Application Security Tools in Text-Based Mode on Non-Windows Platforms

You perform a text-based installation on the command line. During the installation, you are prompted for information required to complete the installation. Text-based installations are not supported on Windows systems.

**Important**

Do not install OpenText™ Application Security Tools in the same directory where OpenText SAST is installed.

To perform a text-based installation of OpenText™ Application Security Tools, run the text-based install command for your operating system as listed in the following table.

| | |
|---|---|
| **Linux** | `./OpenText_Application_Security_Tools_linux-x64_<version>.run --mode text`<br>or<br>`./OpenText_Application_Security_Tools_linux-arm64_<version>.run --mode text` |
| **macOS** | You must uncompress the provided ZIP file before you run the command.<br>`OpenText_Application_Security_Tools_osx-x64_<version>.app/Contents/`<br>MacOS/installbuilder.sh --mode text<br>or<br>`OpenText_Application_Security_Tools_osx-arm64_<version>.app/Contents/`<br>MacOS/installbuilder.sh --mode text |

# 1.2.4.4. Adding Trusted Certificates

Connection from the OpenText SAST applications and tools to other Fortify products and external systems might require communication over HTTPS. Some examples include:

- The OpenText SAST applications and tools such as Fortify Audit Workbench, Fortify Extension for Visual Studio, and Fortify Scan Wizard typically require an HTTPS connection to communicate with Application Security. By default, these tools do not trust self- or locally-signed certificates.
- OpenText SAST configured as a ScanCentral SAST sensor uses an HTTPS connection to communicate with the Controller.

When using HTTPS, OpenText SAST applications and tools will by default apply standard checks to the presented SSL server certificate, including a check to determine if the certificate is trusted. If your organization runs its own certificate authority (CA) and the OpenText SAST applications and tools need to trust connections where the server presents a certificate issued by this CA, you must configure the OpenText SAST applications and tools to trust the CA. Otherwise, the use of HTTPS connections might fail.

You must add the trusted certificate of the CA to the OpenText™ Application Security Tools keystore. The OpenText™ Application Security Tools keystore is in the `<tools_install_dir>/jre/lib/security/cacerts` file. You can use the keytool command to add the trusted certificate to the keystore.

To add a trusted certificate to the OpenText™ Application Security Tools keystore:

1. Open a command prompt, and then run the following command:

   ```
   <tools_install_dir>/jre/bin/keytool -importcert -alias <alias_name> -cacerts -file <cert_file>
   ```

   where:

   - `<alias_name>` is a unique name for the certificate you are adding.
   - `<cert_file>` is the name of the file containing the trusted root certificate in PEM or DER format.

2. Enter the keystore password.

   **Note**

   The default password is `changeit`.

3. When prompted to trust this certificate, select **yes**.

# 1.2.5. About Upgrading OpenText Application Security Tools

To upgrade OpenText™ Application Security Tools, install the new version in a different location than where your current version is installed and choose to migrate settings from the previous installation. This migration preserves and updates the OpenText™ Application Security Tools artifact files located in the `<tools_install_dir>/Core/config` directory.

If you choose not to migrate any settings from a previous release, OpenText recommends that you save a backup of the following data if it has been modified:

- `<tools_install_dir>/Core/config/CustomExternalMetadata` folder
- `<tools_install_dir>/Core/config/server.properties` file
- `<tools_install_dir>/Core/config/fortify.properties` file

After you install the new version, you can uninstall the previous version. For more information, see About Uninstalling Application Security.

**Important**

The ScanCentral SAST client is no longer included in the OpenText™ Application Security Tools installer.

# 1.2.5.1. Upgrading the Fortify Scan Wizard

When you upgrade the OpenText Fortify Scan Wizard in a macOS ARM64 platform to version 25.4.0 or later, you must run the following command and re-launch the Fortify Scan Wizard:

```
/usr/libexec/PlistBuddy -c "Delete :\"Architectures for arm64\":com.fortify.scanwizard"
~/Library/Preferences/com.apple.LaunchServices/com.apple.LaunchServices.plist && sudo reboot
```

# 1.2.5.2. Upgrading the Fortify Extension for Visual Studio

If you have administrative privileges and are upgrading from a previous version of the OpenText™ Application Security Tools for any supported version of Visual Studio, the installer will overwrite the existing Fortify Extension for Visual Studio. If the previous version was installed without administrative privileges, the installer will also overwrite the existing Fortify Extension for Visual Studio without requiring administrative privileges.

**Note**

If you do not have administrative privileges and you are upgrading the Fortify Extension for Visual Studio that was previously installed using an administrative privileged user account, you must first uninstall the Fortify Extension for Visual Studio from Visual Studio using an administrative privilege account.

# 1.2.6. About Uninstalling OpenText™ Application Security Tools

This section describes how to uninstall OpenText SAST applications and tools. You can use the standard install wizard, or you can perform the uninstallation silently. You can also perform a text-based uninstallation on non-Windows systems.

This section contains the following topics:

# 1.2.6.1. Uninstalling OpenText™ Application Security Tools

To uninstall OpenText™ Application Security Tools:

1. Run the uninstall command located in the `<tools_install_dir>` for your operating system:

| | |
|---|---|
| **Windows** | `Uninstall_OpenTextApplicationSecurityTools_<version>.exe`<br>Alternatively, you can uninstall the application from the Windows interface. See the Microsoft documentation for instructions. |
| **Linux** | `Uninstall_OpenTextApplicationSecurityTools_<version>` |
| **macOS** | `Uninstall_OpenTextApplicationSecurityTools_<version>.app` |

2. You are prompted to indicate whether to remove the entire application or individual components. Make your selection, and then click **Next**.

   If you are uninstalling specific components, select the components to remove on the Select Components to Uninstall page, and then click **Next**.

3. You are prompted to indicate whether to remove all application settings. Do one of the following:

   - Click **Yes** to remove the application setting folders for the applications installed with the version of OpenText™ Application Security Tools that you are uninstalling.
   - Click **No** to retain the application settings on your system.

# 1.2.6.2. Uninstalling OpenText™ Application Security Tools Silently

To uninstall OpenText™ Application Security Tools silently:

1. Navigate to the installation directory.
2. Type one of the following commands based on your operating system:

| | |
|---|---|
| **Windows** | `Uninstall_OpenTextApplicationSecurityTools_<version>.exe --mode unattended` |
| **Linux** | `./Uninstall_OpenTextApplicationSecurityTools_<version> --mode unattended` |
| **macOS** | `Uninstall_OpenTextApplicationSecurityTools_<version>.app/Contents/MacOS/installbuilder.sh` --mode unattended |

**Note**

The uninstaller removes the application setting folders for the applications installed with the version of OpenText™ Application Security Tools that you are uninstalling.

# 1.2.6.3. Uninstalling OpenText™ Application Security Tools in Text-Based Mode on Non-Windows Platforms

To uninstall OpenText™ Application Security Tools in text-based mode, run the text-based install command for your operating system, as follows:

1. Navigate to the installation directory.
2. Type one of the following commands based on your operating system:

| | |
|---|---|
| **Linux** | `./Uninstall_OpenTextApplicationSecurityTools_<version> --mode text` |
| **macOS** | `Uninstall_OpenTextApplicationSecurityTools_<version>.app/Contents/MacOS/installbuilder.sh --mode text` |

# 1.2.7. Samples

The OpenText™ Application Security Tools installation includes (optional) sample bug tracker plugins, an analysis results file that was scanned with OpenText SAST, and more. The following table describes the samples in the `<tools_install_dir>/Samples` folder.

| Folder Name | Description |
|---|---|
| `advanced` | Javadoc for `public-api` |
| `bugtrackers` | Source code for supported bug tracker plugins |
| `fortifyclient` | Source code for the REST API-based client to securely transfer objects to and from Application Security |
| `fprs` | Sample Fortify Project Results (FPR) file from the analysis of a WebGoat project |

# 1.2.8. Locating Log Files

By default, log files for OpenText SAST applications and tools are written to the following directory:

- Windows: `C:\Users\<username>\AppData\Local\Fortify\<tool_name>-<version>\log`
- Non-Windows: `<userhome>/.fortify/<tool_name>-<version>/log`

The following table lists log file directory associated with each OpenText SAST application and command-line tool.

| **Application / Tool** | **Log File Directory** |
|---|---|
| Fortify Audit Workbench | `AWB-<version>` |
| Fortify Plugin for Eclipse | `Eclipse.Plugin-<version>` |
| Fortify Analysis Plugin for IntelliJ IDEA and Android Studio | `IntelliJAnalysis-<version>` |
| Fortify Extension for Visual Studio | `VS<VSversion>-<version>` |
| Fortify Scan Wizard | `ScanWizard-<version>` |
| Fortify Custom Rules Editor | `CRE-<version>` |
| ScanCentral SAST client | `scancentral-<version>` |
| BIRTReportGenerator | `BIRT-<version>` |
| ReportGenerator | `ReportCommandlineInterface-<version>` |
| fortifyclient | `FortifyClient-<version>` |
| FPRUtility | `FPRCommandlineInterface-<version>` |

# 1.2.9. Related documents

This topic describes documents that provide information about OpenText Application Security products.

## All products

The following documents provide general information for all products. Unless otherwise noted, these documents are available on the Product Documentation website for each product.

| Document / file name | Description |
|---|---|
| *About OpenText Application Security Software Documentation*<br>appsec-docs-n-*<version>*.pdf | This paper provides information about how to access OpenText Application Security product documentation.<br><br>**Note**<br>This document is included only with the product download. |
| *OpenText™ Application Security System Requirements*<br>appsec-sr-*<version>*.pdf | This document provides the details about the environments and products supported for this version of OpenText Application Security. |
| *What's New in OpenText Application Security<version>*<br>appsec-wn-*<version>*.pdf | This document describes the new features in OpenText Application Security products. |
| *OpenText Application Security Release Notes*<br>appsec-rn-*<version>*.pdf | This document provides an overview of the changes made to OpenText Application Security for this release and important information not included elsewhere in the product documentation. |

## ScanCentral SAST

The following document provides information about ScanCentral SAST. This document is available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-software-security-center.

| Document / file name | Description |
|---|---|
| *OpenText™ ScanCentral SAST Installation, Configuration, and Usage Guide*<br>sc-sast-ugd-*<version>*.pdf | This document provides information about how to install, configure, and use ScanCentral SAST to streamline the static code analysis process. It is written for anyone who intends to install, configure, or use ScanCentral SAST to offload the resource-intensive translation and scanning phases of their OpenText SAST process. |

## Application Security

The following document provides information about OpenText Application Security (Software Security Center). This document is available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-software-security-center.

| Document / file name | Description |
|---|---|

| Document / file name | Description |
|---|---|
| *OpenText™ Application Security User Guide*<br>ssc-ugd-*<version>*.pdf | This document provides Application Security users with detailed information about how to deploy and use Application Security. It provides all the information you need to deploy, configure, and use Application Security.<br>It is intended for use by system and instance administrators, database administrators (DBAs), enterprise security leads, development team managers, and developers. Application Security provides security team leads with a high-level overview of the history and status of a project. |

# OpenText SAST

The following documents provide information about OpenText SAST (Fortify Static Code Analyzer). Unless otherwise noted, these documents are available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-static-code.

| Document / file name | Description |
|---|---|
| *OpenText™ Static Application Security Testing User Guide*<br>sast-ugd-*<version>*.pdf | This document describes how to install and use OpenText SAST to scan code on many of the major programming platforms. It is intended for people responsible for security audits and secure coding. |
| *OpenText™ Static Application Security Testing Custom Rules Guide*<br>sast-cr-ugd-*<version>*.zip | This document provides the information that you need to create custom rules for OpenText SAST. This guide includes examples that apply rule-writing concepts to real-world security issues.<br>**Note**<br>This document is included only with the product download. |
| *OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide*<br>lim-ugd-*<version>*.pdf | This document describes how to install, configure, and use the Fortify License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform. |

# OpenText Application Security Tools

The following documents provide information about OpenText Application Security Tools. These documents are available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-static-code-analyzer-and-tools.

| Document / file name | Description |
|---|---|
| *OpenText™ Application Security Tools Guide*<br>sast-tgd-*<version>*.pdf | This document describes how to install application security tools. It provides an overview of the applications and command-line tools that enable you to scan your code with OpenText SAST, review analysis results, work with analysis results files, and more. |
| *OpenText™ Fortify Audit Workbench User Guide*<br>awb-ugd-*<version>*.pdf | This document describes how to use Fortify Audit Workbench to scan software projects and audit analysis results. This guide also includes how to integrate with bug trackers, produce reports, and perform collaborative auditing. |
| *OpenText™ Fortify Plugin for Eclipse User Guide*<br>ep-udg-*<version>*.pdf | This document provides information about how to install and use the Fortify Plugin for Eclipse to analyze and audit your code. |

| | |
|---|---|
| OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studio User Guide iap-udg-*<version>*.pdf | This document describes how to install and use the Fortify Analysis Plugin for IntelliJ IDEA and Android Studio to analyze your code and optionally upload the results to Application Security. |
| *OpenText™ Fortify Extension for Visual Studio User Guide* vse-ugd-*<version>*.pdf | This document provides information about how to install and use the Fortify Extension for Visual Studio to analyze, audit, and remediate your code to resolve security-related issues in solutions and projects. |

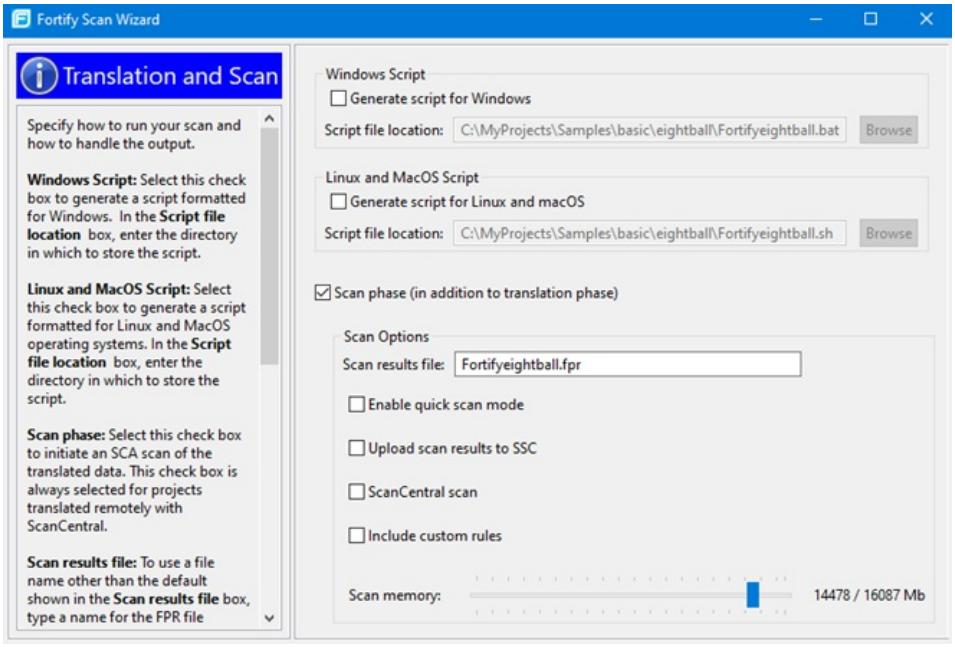
# 1.3. Fortify Scan Wizard

Fortify Scan Wizard is an application with a graphical interface that enables you to easily generate a script to perform OpenText SAST commands for Windows, Linux, and macOS systems. You can run the generated script to analyze your code with OpenText SAST. You can specify to run your analysis locally or use ScanCentral SAST to run all or part of the analysis remotely.

This section contains the following topics:

# 1.3.1. Preparing to use Fortify Scan Wizard

Fortify Scan Wizard uses the information you provide to create a script with the commands for OpenText SAST to scan project code and optionally upload the analysis results to Application Security. You can use Fortify Scan Wizard to create a script that runs your scans locally or sends them to ScanCentral SAST for all or part of the analysis.




To use Fortify Scan Wizard, you need access to the build directory of the projects you want to scan. The following table describes some of the required information you will need, depending on how you will analyze the project and if you want to upload the scan results to Application Security.

**Important**

If Application Security or the ScanCentral SAST Controller uses an SSL connection from an internal certificate authority or a self-signed certificate, you must add the certificate to the Java keystore for OpenText SAST (see the *OpenText™ Static Application Security Testing User Guide*).

| Task | Requirements |
|---|---|
| Perform a local analysis with OpenText SAST | • OpenText SAST installed on the system where the generated script will be run. You can generate the script on a different platform without OpenText SAST, and then transfer the script to the system where it will be run. |

| | |
|---|---|
| Perform a remote analysis (translation and scan phases) with ScanCentral SAST | • Either a ScanCentral SAST client installed with the OpenText™ Application Security Tools installation or a standalone ScanCentral SAST client installation (see the *OpenText™ ScanCentral SAST Installation, Configuration, and Usage Guide* for instructions)<br><br>**Important**<br>The ScanCentral SAST client is no longer included in the OpenText SAST installer.<br><br>• A ScanCentral SAST Controller URL<br><br>**Note**<br>If you are also uploading analysis results to Application Security, then you do not need to specify a Controller URL. The ScanCentral SAST that is integrated with the Application Security server is used in this case.<br><br>• Your project must be in a language that ScanCentral SAST supports for translation. See the *OpenText™ Application Security System Requirements* for a list of supported languages. |
| Perform a local OpenText SAST translation and a remote scan with ScanCentral SAST | • A ScanCentral SAST client installed with the OpenText™ Application Security Tools installation or a standalone ScanCentral SAST client installation<br>• A ScanCentral SAST Controller URL<br>• A Source Analyzer Path to the OpenText SAST `sourceanalyzer.exe` file. |
| Upload analysis results to Application Security | • An Application Security server URL<br><br>**Note**<br>If you are using ScanCentral SAST, the Application Security server must be integrated with the ScanCentral SAST Controller.<br><br>• Your Application Security login credentials<br><br>**Note**<br>If you do not have Application Security login credentials, you must have an application name and version that exists in Application Security.<br><br>• An authentication token of type ToolsConnectToken<br><br>**Note**<br>If you do not have a token, you can use Fortify Scan Wizard to generate one. To do this, you must have Application Security login credentials. |

**Important**

If you generate a script for a Windows system, you cannot run that script on a non-Windows system. Likewise, if you generate a script for a non-Windows system, you cannot run it on a Windows system.

# 1.3.2. Supported file extensions for languages

The following file extensions are supported for the languages:

| Language | File extension |
|---|---|
| ABAP | `.abap` |
| ASP | `.asp` |
| ColdFusion | `.cfm`, `.cfml`, `.cfc` |
| Flex/ActionScript | `.mxml`, `.as` |
| Objective-C | `project.pbxproj` |
| C++ | `makefile` |
| Java | `.java`, `.properties`, `.ini` |
| Java bytecode | `.jar`, `.class` |
| JavaScript/TypeScript | `.js`, `.ts` |
| .NET | `.aspx`, `.exe`, `.dll`, `.mod`, `.mdl`, `.master` |
| JSP | `.jsp`, `.jspx`, `.tag`, `.tagx`, `.xhtml`, `.faces`, `.jsff` |
| PHP | `.php`, `.ctp` |
| Python | `.py` |
| SQL | `.sql`, `.pks`, `.pkh`, `.pkb` |
| Visual Basic | `.vbs`, `.bas`, `.frm`, `.ctl`, `.cls` |
| XML/HTML | `.xml`, `.xsd`, `.xmi`, `.wsdd`, `.config`, `.htm`, `.html` |

# 1.3.3. Supported file extensions in builds tools

The following file extensions are supported for the builds tools:

| Build tool | File extension |
| --- | --- |
| Ant | `build.xml` |
| Maven | `pom.xml` |
| Visual Studio | `.sln` files |

# 1.3.4. Starting Fortify Scan Wizard

To start Fortify Scan Wizard, do one of the following, based on your operating system:

- On Windows, select **Start > All apps > Fortify Applications and Tools *<version>* > Scan Wizard**.

  You can also open a Command Prompt window, and then type `scanwizard`.

- On Linux, navigate to the `*<tools_install_dir>*/bin` directory, and then run `ScanWizard` from the command line.
- On macOS, navigate to the `*<tools_install_dir>*` directory, and then double-click the `ScanWizard.app` icon.

# 1.4. Command-Line Tools

This section describes the tools that you can run from a Command Prompt window.

This section contains the following topics:

# 1.4.1. Generating Analysis Reports from the Command Line

There are two command-line tools that you can use to generate analysis reports:

- BIRTReportGenerator—Generates issue reports from FPR files that are based on the Business Intelligence and Reporting Technology (BIRT) system.

  **Note**

  To generate BIRT reports on a Linux system running OpenJDK, you must install fontconfig, DejaVu Sans fonts, and DejaVu Serif fonts.

- ReportGenerator—Generates legacy reports from FPR files. You can specify a report template or use the default report template. See the *OpenText™ Fortify Audit Workbench User Guide* for a description of the available report templates.

This section contains the following topics:

# 1.4.1.1. Generating Issue Reports

Use the BIRTReportGenerator command-line tool to generate issue reports that are based on the BIRT system. The basic command-line syntax to generate an issue report is:

```
BIRTReportGenerator -template <template_name>
-source <audited_proj>.fpr -format <format>
-output <report_file_name>
```

The following is an example of how to generate an OWASP Top 10 2021 report with additional options:

```
BIRTReportGenerator -template "owasp top 10" -source auditedProj.fpr
-format pdf -ShowSuppressed --Version "owasp top 10 2021"
--UseFortifyPriorityOrder -output MyOWASP_Top10_Report.pdf
```

**See Also**

BIRTReportGenerator Command-Line Options

Troubleshooting BIRTReportGenerator

# 1.4.1.1.1. BIRTReportGenerator Command-Line Options

The following table describes the BIRTReportGenerator options.

| BIRTReportGenerator Option | Description |
|---|---|
| `-template <template_name>` | (Required) Specifies the report template name. The valid values for `<template_name>` are `"CWE Top 25"`, `"CWE/SANS Top 25"`, `"Developer Workbook"`, `"DISA CCI 2"`, `"DISA STIG"`, `"FISMA Compliance"`, `GDPR`, `MISRA`, `"OWASP API Top 10"`, `"OWASP ASVS 5.0"`, `"OWASP MASVS 2.0"`, `"OWASP Mobile Top 10"`, `"OWASP Top 10"`, `"PCI DSS Compliance"`, and `"PCI SSF Compliance"`.<br><br>**Note**<br>You only need to enclose the report template name in quotes if the *<template_name>* includes a space. The template name values are case-insensitive. |
| `-source <audited_proj>.fpr` | (Required) Specifies the audited project on which to base the report. |
| `-format pdf \| doc \| html` | (Required) Specifies the generated report format.<br><br>**Note**<br>The format values are case-insensitive. |
| `-output <report_file.***>` | (Required) Specifies the file to which the report is written.<br><br>**Note**<br>If you specify a file that already exists, that file is overwritten. |
| `-searchQuery <query>` | Specifies a search query to filter issues before generating the report. For example:<br><br>`-searchQuery audited:false`<br><br>For a description of the search query syntax, see the *OpenText™ Fortify Audit Workbench User Guide*. |
| `-ShowSuppressed` | Include issues that are marked as suppressed. |
| `-ShowRemoved` | Include issues that are marked as removed. |
| `-ShowHidden` | Include issues that are marked as hidden. |
| `-filterSet <filterset_name>` | Specifies a filter set to use to generate the report (for example, `-filterSet "Quick View"`). |

| | |
|---|---|
| `--Version <version>` | Specifies the version for the template. The template version values are case-insensitive.<br><br>**Note**<br>• Templates that are not listed here have only one version available.<br>• If you do not specify a version and multiple versions are available, BIRTReportGenerator uses the most recent version based on the external metadata used when the FPR was created.<br>• The BIRTReportGenerator help displays current report versions. OpenText periodically deprecates older report versions, however these versions are still available for FPR files that were created before the report version was deprecated.<br><br>The valid values for the template versions are:<br>• For the "CWE Top 25" template, the version is `"CWE Top 25 <version>"` (for example, `"CWE Top 25 2024"`)<br>• For the "CWE/SANS Top 25" template, the version is `"<version> CWE/SANS Top 25"` (for example, `"2011 CWE/SANS Top 25"`)<br>• For the "DISA STIG" template, the version is `"DISA STIG <version>"` (for example, `"DISA STIG 6.3"`)<br>• For the "FISMA Compliance" template, the version is `"NIST 800-53 Rev <version>"` (for example, `"NIST 800-53 Rev 5"`)<br>• For the MISRA template, the available versions are `"MISRA C 2023"` or `"MISRA C++ 2008"`<br>• For the "OWASP Mobile Top 10" template, the version is `"OWASP Mobile Top 10 <version>"` (for example, `"OWASP Mobile Top 10 2024"`)<br>• For the "OWASP Top 10" template, the version is `"OWASP Top 10 <version>"` (for example, `"OWASP Top 10 2021"`)<br>• For the "PCI DSS Compliance" template, the version is `"PCI <version>"` (for example, `"PCI 4.0.1"`)<br>• For the "PCI SSF Compliance" template, the version is `"PCI SSF <version>"` (for example, `"PCI SSF 1.2"`) |
| `--IncludeDescOfKeyTerminology` | Include the *Description of Key Terminology* section in the report. |
| `--IncludeAboutFortify` | Include the *About Fortify Solutions* section in the report. |
| `--SecurityIssueDetails` | Provide detailed descriptions of reported issues. This option is not available for the Developer Workbook template. |
| `--UseFortifyPriorityOrder` | Use Fortify Priority Order instead of folder names to categorize issues. This option is not available for the Developer Workbook and PCI Compliance templates. |
| `-h` \| `-help` | Displays detailed information about the options. |
| `-debug` | Displays debug information that can be helpful to troubleshoot issues with BIRTReportGenerator. |

# 1.4.1.1.2. Troubleshooting BIRTReportGenerator

Occasionally, you might encounter an out of memory error when you generate a report. You might see a message similar to the following in the command-line output:

```
java.lang.OutOfMemoryError: GC overhead limit exceeded
```

To increase the memory allocated for BIRTReportGenerator, add the `-Xmx` option to the BIRTReportGenerator command. In the following example, 32 GB is allocated to BIRTReportGenerator to run a report:

```
BIRTReportGenerator -template "DISA STIG" -source myproject.fpr -format PDF -output mypr
oject_report.pdf -Xmx32G
```

# 1.4.1.2. Generating a Legacy Analysis Report

Use the ReportGenerator command-line tool to generate legacy reports. The legacy reports include user-configurable report templates. The basic command-line syntax to generate a legacy analysis report is:

```
ReportGenerator -source <audited_proj>.fpr -format <format> -f <report_file_name>
```

The following is an example of how to generate a PDF report using the Fortify Scan Summary template and additional options:

```
ReportGenerator -source auditedProj.fpr -format pdf -template ScanReport.xml -showSuppre
ssed -user Alex -f MyFortifyReport.pdf
```

# 1.4.1.2.1. ReportGenerator Command-Line Options

The following table describes the ReportGenerator options.

| ReportGenerator Option | Description |
|---|---|
| `-source <audited_proj>.fpr` | (Required) Specifies the audited project on which to base the report. |
| `-format pdf \| xml` | (Required) Specifies the generated report format. |
| `-f <report_file.***>` | (Required) Specifies the file to which the report is written.<br><br>**Note**<br>If you specify a file that already exists, that file is overwritten. |
| `-template <template_name>` | Specifies the report template. If not specified, ReportGenerator uses the default template. The default template is located in `<tools_install_dir>/Core/config/reports/DefaultReportDefinition.xml`.<br><br>**Note**<br>Enclose the *<template_name>* in quotes if it contains any spaces.<br><br>See the *OpenText™ Fortify Audit Workbench User Guide* for a description of the available report templates and how to customize them. |
| `-user <username>` | Specifies a user name to add to the report. |
| `-showSuppressed` | Include issues marked as suppressed. |
| `-showRemoved` | Include issues marked as removed. |
| `-showHidden` | Include issues marked as hidden. |
| `-filterSet <filterset_name>` | Specifies a filter set to use to generate the report (for example, `-filterset "Quick View"`). |
| `-verbose` | Displays status messages to the console. |
| `-debug` | Displays debug information that can be helpful to troubleshoot issues with ReportGenerator. |
| `-h` | Displays detailed information about the options. |

# 1.4.2. Working with FPR Files from the Command Line

Use the FPRUtility command-line tool located in `<tools_install_dir>/bin` to perform the following tasks:

- Merging FPR Files
- Displaying Analysis Results Information from an FPR File
- Extracting a Source Archive from an FPR File
- Altering FPR Files
- Allocating More Memory for FPRUtility

# 1.4.2.1. Merging FPR Files

The FPRUtility `-merge` option combines the analysis results from two FPR files into a single FPR file. The values of the primary project are used to resolve conflicts. When you merge two FPR files, copies of both the primary analysis results and the secondary analysis results are stored in the merged FPR. When you open a merged FPR in Fortify Audit Workbench or Application Security, *removed issues* are determined as those that exist in the secondary analysis results but not in the primary analysis results. Similarly, *new issues* are those that exist in the primary analysis results, but not in the secondary analysis results.

To merge FPR files:

```
FPRUtility -merge -project <primary>.fpr -source <secondary>.fpr \
-f <merged>.fpr
```

To merge FPR files and set instance ID migrator options:

```
FPRUtility -merge -project <primary>.fpr -source <secondary>.fpr \
-f <merged>.fpr -iidmigratorOptions "<iidmigrator_options>"
```

## FPRUtility Data Merge Options

The following table lists the FPRUtility options that apply to merging data.

| FPRUtility Option | Description |
|---|---|
| `-merge` | Merges the specified project and source FPR files. |
| `-project <primary>.fpr` | Specifies the primary FPR file to merge. Conflicts are resolved using the values in this file. |
| `-source <secondary>.fpr` | Specifies the secondary FPR file to merge. The primary project overrides values if conflicts exist. |
| `-f <merged>.fpr` | Specifies the name of the merged FPR file to contain the result of the merged files.<br>**Note**<br>When you specify this option, neither of the original FPR files are modified. If you do not use this option, the primary FPR is overwritten with the merged results. |
| `-forceMigration` | Forces the migration, even if OpenText SAST and the Rulepack versions of the two projects are the same. |
| `-ignoreAnalysisDates` | Specifies to ignore the analysis dates in the primary and secondary FPR files for the merge. Otherwise, the secondary FPR is always updated with the primary FPR . |
| `-useSourceIssueTemplate` | Specifies to use the filter sets and folders from the issue template in the secondary FPR. |
| `-useMigrationFile <mapping_file>` | Specifies an instance ID mapping file. This enables you to modify mappings manually rather than using the migration results. Supply your own instance ID mapping file. |

| | |
|---|---|
| `-iidmigratorOptions <iidmigrator_options>` | Specifies instance ID migrator options. Separate included options with spaces and enclosed them in quotes. Some valid options are:<br>• `-i` provides a case-sensitive file name comparison of the merged files<br>• `-u <scheme_file>` tells iidmigrator to read the matching scheme from `<scheme_file>` for instance ID migration<br>**Note**<br>Wrap `<-iidmigrator_options>` in single quotes (`'-u <scheme_file>'`) when working from a Cygwin command prompt.<br>Windows example:<br>`FPRUtility -merge -project <primary>.fpr` -source *<secondary>*.fpr -f *<merged>*.fpr -iidmigratorOptions "-u scheme_file" |
| `-debug` | Displays debug information that can be helpful to troubleshoot issues with FPRUtility. |

# FPRUtility Data Merge Exit Codes

Upon completion of the `-merge` command, FPRUtility provides one of the exit codes described in the following table.

| Exit Code | Description |
|---|---|
| 0 | The merge completed successfully. |
| 5 | The merge failed. |

# 1.4.2.2. Displaying Analysis Results Information from an FPR File

The FPRUtility `-information` option displays information about the analysis results. You can obtain information to:

- Validate signatures
- Examine any errors associated with the FPR
- Obtain the number of issues for each analyzer, vulnerability category, or custom grouping
- Obtain lists of issues (including some basic information). You can filter these lists.
- Obtain list of issues (with additional metadata). You can filter these lists.
- Obtain the list of analyzed files and the number of lines of code (LOC) for each file. You can also compare the LOC with another FPR.

To display signature information for the analysis:

```
FPRUtility -information -signature -project <project>.fpr -f <output>.txt
```

To display a full analysis error report for the FPR:

```
FPRUtility -information -errors -project <project>.fpr -f <output>.txt
```

To display the number of issues per vulnerability category or analyzer:

```
FPRUtility -information -categoryIssueCounts -project <project>.fpr
FPRUtility -information -analyzerIssueCounts -project <project>.fpr
```

To display the number of issues for a custom grouping based on a search:

```
FPRUtility -information -search -query <search_expression> \
[-categoryIssueCounts] [-analyzerIssueCounts] \
[-includeSuppressed] [-includeRemoved] \
-project <project>.fpr -f <output>.txt
```

**Note**

By default, the result does not include suppressed and removed issues. To include suppressed or removed issues, use the `-includeSuppressed` or `-includeRemoved` options.

To display information for issues in CSV format:

```
FPRUtility -information -listIssues \
-search [-queryAll | -query <search_expression>] \
[-categoryIssueCounts] [-analyzerIssueCouts] \
[-includeSuppressed] [-includeRemoved] \
-project <project>.fpr -f <output>.csv -outputFormat CSV
```

To display information for all issues from the most recent scan (excluding suppressed and removed issues) using the Quick View filter set:

```
FPRUtility -information -listIssues \
-search -queryAllExistingUnsuppressed \
-filterSet "Quick View" \
[-categoryIssueCounts] [-analyzerIssueCouts] \
-project <project>.fpr -f <output>.txt
```

To display a comparison of the number of lines of code for analyzed files in two FPRs:

```
FPRUtility -information -loc -project <project>.fpr \
-compareTo <oldproject>.fpr -f <output>.txt
```

# FPRUtility Information Options

The following table lists the FPRUtility options that apply to project information. Specify one of the following options to indicate what information to display with the `-information` command:

| FPRUtility Option | Description |
|---|---|
| `-information` | Required. Displays information for the project. |
| `-signature` | Displays the signature for analysis results and rules. |
| `-mappings` | Displays the migration mappings report. |
| `-errors` | Displays a full error report for the FPR. |
| `-versions` | Displays the OpenText SAST and OpenText Secure Coding Rulepacks versions used in the static scan. |
| `-functionsMeta` | Displays all functions that the static analyzer encountered in CSV format. To filter which functions are displayed, include `-excludeCoveredByRules`, and `-excludeFunctionsWithSource`. |
| `-categoryIssueCounts` | Displays the number of issues for each vulnerability category. |
| `-analyzerIssueCounts` | Displays the number of issues for each analyzer. |
| `-search <query_option>` | • Use `-search -query <search_expression>` to display the number of issues in the result of your specified search expression. To display the number of issues per vulnerability category or analyzer, add the optional `-categoryIssueCounts` and `-analyzerIssueCounts` options to the search option. Use the `-includeSuppressed` and `-includeRemoved` options to include suppressed or removed issues.<br>• Use `-search -queryAll` to search all the issues in the FPR including suppressed and removed issues.<br>• Use `-search -queryAllExistingUnsuppressed` to search all the issues in the FPR excluding suppressed and removed issues. |

| | |
|---|---|
| `-loc` | Displays the list of analyzed files each with the number of lines of code (LOC) in the following format:<br>`<filename>: <total_loc> (<executable_loc>)`<br>where *<total_loc>* is the approximate number of lines that contain code constructs (comments are excluded).<br><br>**Note**<br>Ignore the *<executable_loc>* metric. It is no longer used.<br>For FPR files created using OpenText SAST version 24.2 and later, the *<executable_loc>* value always matches the *<total_loc>* value. Also, *<total_loc>* includes all lines of code (including comments and blank lines).<br><br>Use `-compareTo <project>.fpr` with this option to compare the number of lines of code with another FPR. The comparison output includes the following information:<br>• `+` indicates new analyzed files<br>• `-` indicates removed analyzed files<br>• `*` indicates files with a different number of lines of code. The difference in the number of lines of code is shown next to the executable LOC number as in (`+`N or `-`N). For example:<br>`* ProjectA/main.jsp: 115 +15 (85 +15)`<br>In the previous example, the comparison shows that the number of lines of code in `main.jsp` is different between the two FPR files. There are 15 additional total LOC. |
| `-project <project>.fpr` | Specifies the FPR from which to extract the results information. |
| `-listIssues` | Displays the location for each issue in one of the following formats:<br>`<sink_filename>:<line_num>` or<br>`<sink_filename>:<line_num>` (`<category>` \| `<analyzer>`)<br>You can also use the `-listIssues` option with `-search` and with both issueCounts grouping options. If you group by `-categoryIssueCounts`, then the output includes (*<analyzer>*) and if you group by `-analyzerIssueCounts`, then the output includes (*<category>*).<br>If you specify the `-outputFormat CSV` option, then each issue is displayed on one line in the format:<br>`"<instanceid>", "<category>", "<sink_filename>:<line_num>", "<analyzer>"` |
| `-listIssuesWithMetadata` | Displays the location for each issue with the following additional metadata:<br>`<audience>, <confidence>, <friority>, <likelihood>, <impact>, <probability>, <accuracy>`<br>Use one of the following format:<br>`<sink_filename>:<line_num>` or<br>`<sink_filename>:<line_num>` (`<category>` \| `<analyzer>`\|`<audience>`\|`<friority>`)<br>You can also use the `-listIssuesWithMetadata` option with `-search` and with both issueCounts grouping options. If you group by `-categoryIssueCounts`, then the output includes (*<analyzer>*) and if you group by `-analyzerIssueCounts`, then the output includes (*<category>*).<br>If you specify the `-outputFormat CSV` option, then each issue is displayed on one line in the format:<br>`"<instanceid>", "<category>", "<audience>", "<confidence>", "<friority>", "<likelihood>", "<impact>", "<probability>", "<accuracy>"`<br>`"<sink_filename>:<line_num>", "<analyzer>"` |
| `-filterSet <filterset_name>` | Displays only the issues and counts that pass the filters specified in the filter set. Filter sets are ignored without this option.<br><br>**Important**<br>You must use `-search` with this option. |
| `-f <output>` | Specifies the output file. The default is `System.out`. |

| | |
|---|---|
| `-outputFormat TEXT \| CSV` | Specifies the output format. The default value is `TEXT`. |
| `-debug` | Displays debug information that can be helpful to troubleshoot issues with FPRUtility. |

# FPRUtility Signature Exit Codes

Upon completion of the `-information -signature` command, FPRUtility provides one of the exit codes described in the following table.

| Exit Code | Description |
|---|---|
| 0 | The project is signed, and all the signatures are valid. |
| 1 | The project is signed, and some, but not all, of the signatures passed the validity test. |
| 2 | The project is signed but none of the signatures are valid. |
| 3 | The project had no signatures to validate. |

# 1.4.2.3. Extracting a Source Archive from an FPR File

The FPRUtility `-sourceArchive` option creates a source archive (FSA) file from a specified FPR file and removes the source code from the FPR file. You can extract the source code from an FPR file, merge an existing source archive (FSA) back into an FPR file, or recover source files from a source archive.

To archive data:

```
FPRUtility -sourceArchive -extract -project <project>.fpr -f <output_archive>.fsa
```

To archive data to a directory:

```
FPRUtility -sourceArchive -extract -project <project>.fpr \
-recoverSourceDirectory -f <output_dir>
```

To add an archive to an FPR file:

```
FPRUtility -sourceArchive -mergeArchive -project <project>.fpr \
-source <old_source_archive>.fsa -f <project_with_archive>.fpr
```

To recover files that are missing from an FPR file:

```
FPRUtility -sourceArchive -fixSecondaryFileSources \
-payload <source_archive>.zip -project <project>.fpr -f <output>.fpr
```

## FPRUtility Source Archive Options

The following table lists the FPRUtility options that apply to working with the source archive.

| FPRUtility Option | Description |
|---|---|
| `-sourceArchive` | Creates an FSA file so that you can extract a source archive. |
| One of:<br>`-extract`<br>-mergeArchive<br>-fixSecondaryFileSources | Use the `-extract` option to extract the contents of the FPR file. |
| | Use the `-mergeArchive` option to merge the contents of the FPR file with an existing archived file (`-source` option). |
| | Use the `-fixSecondaryFileSources` option to recover source files from a source archive (`-payload` option) missing from an FPR file. |
| `-project <project>.fpr` | Specifies the FPR to archive. |
| `-recoverSourceDirectory` | Use with the `-extract` option to extract the source as a directory with restored source files. |
| `-source <old_source_archive>.fsa` | Specifies the name of the existing archive. Use only if you are merging an FPR file with an existing archive (`-mergeArchive` option). |

| | |
|---|---|
| `-payload <source_archive>.zip` | Use with the `-fixSecondaryFileSources` option to specify the source archive from which to recover source files. |
| `-f <project_with_archive>.fpr \| <output_archive>`.fsa \| *<output_dir>* | Specifies the output file. You can generate an FPR, a directory, or an FSA file. |
| `-debug` | Displays debug information that can be helpful to troubleshoot issues with FPRUtility. |

# 1.4.2.4. Altering FPR Files

Use the FPRUtility `-trimToLastScan` option to remove the previous scan results from a merged project (FPR). This reduces the size of the FPR file when you no longer need the previous scan results. This can also reduce the time it takes to open an FPR in Fortify Audit Workbench.

To remove the previous scan from the FPR:

```
FPRUtility -trimToLastScan -project <merged_project>.fpr [-f <output>.fpr]
```

## FPRUtility Alter FPR File Options

| FPRUtility Option | Description |
|---|---|
| `-trimToLastScan` | Removes the previous scan results from a merged project. |
| `-project <merged_project>.fpr` | Specifies the merged FPR to alter. If this project is not a merged project, then the FPR file remains unchanged. |
| `-f <output>.fpr` | Specifies the name of the altered output file.<br>If you do not specify this option, then the merged FPR is altered. |

# 1.4.2.5. Allocating More Memory for FPRUtility

Performing tasks with large and complex FPR files might trigger out-of-memory errors. By default, 1000 MB is allocated for FPRUtility. To increase the memory, add the `-Xmx` option to the command line. For example, to allocate 2 GB for FPRUtility, use the following command:

```
FPRUtility -Xmx2G -merge -project <primary>.fpr -source <secondary>.fpr \
-f <output>.fpr
```

# 1.5. Configuration Options

The OpenText™ Application Security Tools installer places a set of properties files on your system. Properties files contain configurable settings for OpenText SAST applications and tools. Some properties described in this chaptersection already exist in the properties file, and some of them you must add yourself. You can modify any of the properties in the configuration file with a text editor.

This section contains the following topics:

# 1.5.1. Properties File Format

In a properties file, each property consists of a pair of strings: the first string is the property name and the second string is the property value.

```
com.fortify.log.console=false
```

As shown above, the property disables console logging. The property name is `com.fortify.log.console` and the value is set to `false`.

# 1.5.2. Configuration Options for Java-Based Applications and IDE Plugins

This section describes the properties to configure the following Java-based OpenText SAST applications.

- Fortify Audit Workbench
- Fortify Custom Rules Editor
- Fortify Plugins for Eclipse, IntelliJ IDEA, and Android Studio

The following table lists the OpenText SAST application acronyms used in this section.

| **Acronym** | **Fortify Application / Plugin / Extension** |
|---|---|
| AWB | Fortify Audit Workbench |
| CRE | Fortify Custom Rules Editor |
| ECP | Fortify Plugin for Eclipse |
| IAP | Fortify Analysis Plugin for IntelliJ IDEA and Android Studio |

# 1.5.2.1. Where to Find the Properties File

The location of the properties file `fortify.properties` varies for the different OpenText SAST applications. The following table provides the location of the properties file for the applications described in this chaptersection.

| Fortify Application | Property File Location |
|---|---|
| AWB, CRE | `<tools_install_dir>/Core/config`<br><br>**Note**<br>After you specify the location of the OpenText SAST executable from Fortify Audit Workbench, the location of the properties file changes to `/Core/config` for AWB. |
| ECP | `/plugins/com.fortify.dev.ide.eclipse_<version>/Core/config`<br>or if Eclipse was installed with an installer:<br>`<userhome>/.p2/pool/plugins/com.fortify.dev.ide.eclipse_<version>/Core/config` |
| IAP | `<IDE_product_plugins_dir>/Core/config`<br>The following is an example location on Windows:<br><br>C:\Users*<username>*\AppData\Roaming\JetBrains\Idea*<version>*\plugins\Fortify\config |

# 1.5.2.2. Java-Based Applications and IDE Plugin Properties

Some properties described in this section already exist in the `fortify.properties` file, and some of them you must add yourself. The colored boxes in the Details column indicate which OpenText SAST applications use the property. To find this properties file for the various products, see Where to Find the Properties File.

The following table describes the properties in the `fortify.properties` file.

| Property | Details |
|---|---|
| com.fortify.audit.ui.DisableAddingFolders | If set to `true`, disables the add folder functionality.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.audit.ui.DisableBugtrackers | If set to `true`, disables bug tracker integration.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.audit.ui.DisableEditingCustomTags | If set to `true`, removes the ability to edit custom tags.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.audit.ui.DisableSuppress | If set to `true`, disables issue suppression.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.AuthenticationKey | Specifies the directory to store the encrypted Application Security authentication token.<br>**Default:** `${com.fortify.WorkingDirectory}/config/tools`<br>**Tools Affected: AWB, ECP, CRE, IAP** |
| com.fortify.awb.Debug | If set to `true`, Fortify Audit Workbench runs in debug mode.<br>**Default:** `false`<br>**Tools Affected: AWB** |
| com.fortify.awb.javaExtensions | Specifies the file extensions (comma-delimited) to treat as Java files during a scan.<br>If this property is empty, Fortify Audit Workbench and the Fortify Plugin for Eclipse recognize .`java`, .`jsp`, and .`jspx` files as Java files. The property only determines whether a project includes Java files and to add Java-specific controls to the Advanced Scan wizard.<br>**Default:** none<br>**Tools Affected: AWB, ECP** |
| com.fortify.awb.forceGCOnProjectClose | If set to `true`, garbage collection is run and heap space is released when you close a project. This reduces the increased Java process memory consumption when working with small FPR files. When Fortify Audit Workbench runs with G1GC garbage collection, the Java process can return free memory back to the operating system when the project is closed.<br>**Default:** `false`<br>**Tools Affected: AWB** |
| com.fortify.awb.LinuxFontAdjust | Specifies the font size to use on Linux platforms. Fortify Audit Workbench adds the specified size to original font size.<br>**Default:** `0`<br>**Tools Affected: AWB, ECP, CRE** |
| com.fortify.awb.MacFontAdjust | Specifies to tune font size for the macOS platform. Fortify Audit Workbench adds the specified size to the original font size.<br>**Default:** `2`<br>**Tools Affected: AWB, ECP, CRE** |
| com.fortify.awb.WindowsFontAdjust | Specifies to tune the font size for the Windows platform. Fortify Audit Workbench adds the specified size to original font size.<br>**Default:** `0`<br>**Tools Affected: AWB, ECP, CRE** |

| | |
|---|---|
| com.fortify.<br>Debug | If set to `true`, runs the OpenText SAST applications in debug mode.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.<br>DisableDescriptionXML<br>Escaping | If set to `true`, disables XML escaping in issue descriptions (for example, changing `&quot;` in XML/FVDL to `"`).<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.<br>DisableExternalEntry<br>Correlation | If set to `true`, parses URL in the ExternalEntries/Entry element in the FVDL file.<br>**Default:** `false`<br><br>`<ExternalEntries>`<br>`<Entry name="HTML Form" type="URL">`<br>`<URL>/auth/PerformChangePass.action</URL>`<br>`<SourceLocation path="pages/content/`<br>`ChangePass.jsp" line="16" lineEnd="16"`<br>`colStart="0" colEnd="0" snippet=`<br>`"1572130B944CEC7A3D98775A499AE8FA#pages/`<br>`content/ChangePass.jsp:16:16"/>`<br>`</Entry>`<br>`</ExternalEntries>`<br><br>**Tools Affected: AWB, ECP** |
| com.fortify.<br>DisableMinVirtCallConfidence<br>Computation | If set to `true`, disables computing minimum virtual call confidence.<br>Fortify Audit Workbench and the Fortify Plugin for Eclipse use this attribute to compute minimum virtual call confidence and enable issue filtering. For example, you can use it to filter out all issues that contain a virtual call with confidence lower than 0.46.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.<br>DisableRemovedIssue<br>Persistance | If set to `true`, disables removed issue persistence (clears removed issues from the FPR file).<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.<br>DisableReportCategory<br>Rendering | If set to `true`, disables rendering issue description into reports.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.<br>DisplayEventID | If set to `true`, displays the event ID in the issue node tooltip in the Issues view.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.<br>eclipse.Debug | If set to `true`, runs the plugin in debug mode.<br>**Default:** `false`<br>**Tools Affected: ECP** |
| com.fortify.<br>InstallationUserName | Specifies the default user name for logging in to Application Security for the first time.<br>**Default:** `${user.name}`<br>**Tools Affected: AWB, ECP, CRE, IAP** |
| com.fortify.<br>locale | Specifies the locale (for rules and metadata only). The possible values are:<br>`en` (English)<br>`es` (Spanish)<br>`ja` (Japanese)<br>`ko` (Korean)<br>`pt_BR` (Brazilian Portuguese)<br>`zh_CN` (Simplified Chinese)<br>`zh_TW` (Traditional Chinese)<br>**Default:** `en`<br>**Tools Affected: AWB, ECP, CRE, IAP** |

| | |
|---|---|
| com.fortify.model.CheckSig | If set to `true`, verifies the signature in the FPR file.<br>If `com.fortify.model.UseIssueParseFilters` is set to `true`, then `com.fortify.model.MinimalLoad` is set to true, `com.fortify.model.IssueCutoffStartIndex` is not null, `com.fortify.model.IssueCutoffEndIndex` is not null, `com.fortify.model.IssueCutoffByCategoryStartIndex` is not null or `com.fortify.model.IssueCutoffByCategoryEndIndex` is not null, `com.fortify.model.CheckSig` is `false`, and the signature in FPRs are not verified.<br>**Default:** `true` (normal) / `false` (minimum load)<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.CustomDescriptionsHeader | Specifies a custom prefix for the description header. It prepends the text in the `Description/Recommendation` header, so that you see "My Recommendations" instead of "Custom Recommendations."<br><br>**Note**<br>To update description headers, OpenText recommends that you use the `<CustomDescriptionRule>` rule with the `<Header>` element text instead.<br><br>**Default:** none<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.DisableChopBuildID | If set to `true`, does not shorten the build ID, even if the build ID exceeds 250 characters.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.DisableContextPool | If set to `true`, disables loading the `ContextPool` section of the FVDL file.<br>You can configure this property if `com.fortify.model.MinimalLoad` is not set to `true`. If `com.fortify.model.MinimalLoad` is set to `true`, then `com.fortify.model.DisableContextPool` is automatically set to `true`.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.DisableDescription | If set to `true`, disables loading the `Description` section from the FVDL file.<br>You can configure this property if `com.fortify.model.MinimalLoad` is not set to `true`. If `com.fortify.model.MinimalLoad` is `true`, then `com.fortify.model.DisableDescription` is automatically set to `true`.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.DisableEngineData | If set to `true`, disables loading the `EngineData` section of the FVDL file to save memory when large FPR files are opened. This data is displayed on the **Analysis Information** tab of **Project Summary** view. The property is useful if too many analysis warnings occur during a scan. However, OpenText recommends that you instead set a limit for `com.fortify.model.MaxEngineErrorCount` to open FPR files that have many OpenText SAST warnings.<br>Also see com.fortify.model.MaxEngineErrorCount<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.DisableProgramInfo | If set to `true`, disables use of the code navigation features in Fortify Audit Workbench.<br>You can configure this property if `com.fortify.model.MinimalLoad` is not `true`. If `com.fortify.model.MinimalLoad` is set to `true`, then this property is automatically set to `true`.<br>Also see com.fortify.model.MinimalLoad<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.DisableProgramPoint | If set to `true`, disables loading of the `ProgramPoint` section from the `runtime.fvdl` file.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |

| | |
|---|---|
| com.fortify.model.DisableReplacementParsing | If set to `true`, disables replacing the conditional description.<br>You can configure this property if `com.fortify.model.MinimalLoad` is not set to `true`. If `com.fortify.model.MinimalLoad` is `true`, then this property is automatically set to `true`.<br>Also see com.fortify.model.MinimalLoad<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.DisableSnippets | If set to `true`, disables loading the `Snippets` section from the FVDL file.<br>You can configure this property if `com.fortify.model.MinimalLoad` is set to `false`. If `com.fortify.model.MinimalLoad` is set to `true`, then `com.fortify.model.DisableSnippets` is automatically set to `true`.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.DisableUnifiedInductions | If set to `true`, disables loading the `UnifiedInductionPool` section from the FVDL file.<br>You can configure this property if `com.fortify.model.MinimalLoad` is not set to `true`. If `com.fortify.model.MinimalLoad` is set to `true`, then `com.fortify.model.DisableUnifiedInductions` is automatically set to `true`.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.DisableUnifiedPool | If set to `true`, disables loading the `UnifiedNodePool` section from the FVDL file.<br>You can configure this property if `com.fortify.model.MinimalLoad` is set to `false`. If `com.fortify.model.MinimalLoad` is `true`, then `com.fortify.model.DisableUnifiedPool` is automatically set to `true`. If the value is not specified or false, this property is set to none.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.DisableUnifiedTrace | If set to `true`, disables loading the `UnifiedTracePool` section from the FVDL file.<br>You can configure this property if `com.fortify.model.MinimalLoad` is not set to `true`. If `com.fortify.model.MinimalLoad` is `true`, then `com.fortify.model.DisableUnifiedTrace` is automatically set to `true`.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.EnableSourceCorrelation | If set to `true`, takes data flow source into consideration for issue correlation. The default is `false` because correlations with runtime results might not be reliable with this setting enabled.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.ExecMemorySetting | Specifies the JVM heap memory size in megabytes that Fortify Audit Workbench uses to start external utilities.<br>**Default:**<br>`600`—iidmigrator<br>`300`—fortifyupdate<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.ForceIIDMigration | If set to `true`, forces running Instance ID migration during a merge.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.FullReportFilenames | If set to `true`, uses the full file name in reports.<br>**Default:** `false`<br>**Tools Affected:** Also used the FPRUtility command-line tool<br>**AWB, ECP** |
| com.fortify.model.IIDmigratorOptions | Specifies iidmigrator options (space-delimited values).<br>**Default:** none<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.IssueCutoffByCategoryStartIndex | Specifies the start index for issue cutoff by category.<br>**Default:** `0`<br>**Tools Affected: AWB, ECP** |

| | |
|---|---|
| com.fortify.model.IssueCutoffByCategoryEndIndex | Specifies the end index for issue cutoff by category.<br>**Default:** `java.lang.Integer.MAX_VALUE`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.IssueCutoffStartIndex | Specifies the start index for issue cutoff. Select the first issue (by number) to load.<br>**Default:** `0`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.IssueCutoffEndIndex | Specifies the end index for issue cutoff. Select the last issue (by number) to load.<br>**Default:** `java.lang.Integer.MAX_VALUE`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.MaxEngineErrorCount | Specifies how many reported OpenText SAST warnings to load. To allow an unlimited number, specify `-1`.<br>OpenText recommends that you keep the default value of `3000` because this can speed up the load time of large FPR files.<br>**Default:** `3000`<br>**Tools Affected:** Also used by FPRUtility<br>**AWB, ECP** |
| com.fortify.model.MergeResolveStrategy | Specifies the merge resolve strategy to one of the following:<br>• `DefaultToMasterValue` (use primary project)<br>• `DefaultToImportValue` (use secondary project)<br>• `NoStrategy` (prompt for project to use)<br>**Default:** `DefaultToMasterValue`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.MinimalLoad | If set to `true`, minimizes the data loaded from an FPR file.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.NProcessingThreads | Specifies the number of threads used to process FPR files.<br>If the `com.fortify.model.PersistDataToDisk` property is set to `true`, this value defaults to one thread.<br>If the number specified exceeds the number of available processors, then OpenText SAST tools use the number of available processors as the number of threads to process FPR files.<br>Also see: com.fortify.model.PersistDataToDisk<br>**Default:** Number of available processors<br>**Tools Affected:** Also used by FPRUtility<br>**AWB, ECP** |
| com.fortify.model.PersistDataToDisk | If set to `true`, enables a persistence strategy to reduce the memory footprint and uses the disk drive to swap FPR data out of memory.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.PersistenceBlockSize | This property specifies the number of attribute values that comprise a single block of attributes. These blocks are cached to disk and read back in as needed. A larger number decreases the total number of cache files, but increases the file size and the amount of memory that is read in each time.<br>**Default:** `250`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.PersistenceQueueCapacity | This property specifies the maximum number of attribute value blocks that can exist in the producer/consumer queue.<br>**Default:** queue is unbounded<br>**Tools Affected: AWB, ECP** |

| | |
|---|---|
| com.fortify.model.PriorityImpactThreshold | Specifies the threshold for issue impact. The valid values are 0.0F–5.0F. If the impact of an issue is greater than or equal to the threshold, the issue is considered High. If the impact of an issue is less than the threshold, the issue is considered Low. Issues are then categorized as follows:<br>• **Critical**—High Impact and High Likelihood<br>• **High**—High Impact and Low Likelihood<br>• **Medium**—Low Impact and High Likelihood<br>• **Low**—Low Impact and Low Likelihood<br>Also see com.fortify.model.PriorityLikelihoodThreshold<br>**Default:** `2.5F`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.PriorityLikelihoodThreshold | Specifies the threshold for issue likelihood. The valid values are 0.0F–5.0F. If the likelihood of an issue is greater than or equal to the threshold, the issue is considered High. If the likelihood of an issue is less than the threshold, the issue is considered Low. Issues are then categorized as follows:<br>• **Critical**—High Impact and High Likelihood<br>• **High**—High Impact and Low Likelihood<br>• **Medium**—Low Impact and High Likelihood<br>• **Low**—Low Impact and Low Likelihood<br>Also see com.fortify.model.PriorityImpactThreshold<br>**Default:** `2.5F`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.report.useSystemLocale | If set to `true`, uses the system locale for report output. If set to `false`, uses `com.fortify.locale` in the `fortify.properties` file. If a value is not specified, the tool uses `java.util.Locale.getDefault()`.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.ReportLineLimit | Specifies the character limit for each issue code snippet in reports.<br>**Default:** `500`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.UseIIDMigrationFile | Specifies the full path of the instance ID migration file to use.<br>**Default:** none<br>**Tools Affected:** Also used by FPRUtility<br>**AWB, ECP** |
| com.fortify.model.UseIssueParseFilters | If set to `true`, respects the settings in the `IssueParseFilters.properties` configuration file. This file is in the following directories:<br>**AWB**—*<tools_install_dir>*/Core/config<br>**ECP**—`/plugins/com.fortify.`dev.ide.eclipse_*<version>*/Core/config<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.model.UseOldIIDMigrationAttributes | If set to `true`, uses attributes of old issues during instance ID migration while merging similar issues of old and new scans.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.RemovedIssuePersistanceLimit | Specifies how many removed issues to keep when you save an FPR.<br>**Default:** `1000`<br>**Tools Affected: AWB, ECP** |
| com.fortify.SCAExecutablePath | Specifies the file path to `sourceanalyzer.exe`.<br>**Tools Affected: AWB, ECP, IAP** |

| | |
|---|---|
| com.fortify.search.defaultSyntaxVer | Specifies whether to use the AND and OR operators in searches. These are enabled in search syntax by default.<br>• To block the use of the AND and OR operators, set the value to `1`.<br>• To use ANDs and ORs without parentheses, set the value to `2`.<br>**Default:** `2`<br>**Tools Affected: AWB, ECP** |
| com.fortify.StoreOriginalDescriptions | If set to `true`, stores original plain text issue descriptions (before parsing) as well as the parsed ones with tags replaced with specific values.<br>**Default:** `false`<br>**Tools Affected: AWB, ECP** |
| com.fortify.taintFlagBlacklist | Specifies taint flags to exclude (comma-delimited values).<br>**Default:** none<br>**Tools Affected: AWB, ECP** |
| com.fortify.tools.iidmigrator.scheme | Set this property to migrate instance IDs created with different versions of OpenText SAST using a custom matching scheme. This is handled by OpenText SAST. If you need a custom matching scheme, contact Customer Support.<br>**Default:** none<br>**Tools Affected: AWB, ECP** |
| com.fortify.UseSourceProjectTemplate | This property determines the issue template to use when merging analysis information from two audit projects. If set to true, it forces the use of filter sets and folders from the issue template associated with the original scan results (secondary project). The issue template from the new scan results (primary project) is used by default.<br>**Default:** `false`<br>**Tools Affected:** Also used by FPRUtility<br>**AWB, ECP** |
| com.fortify.WorkingDirectory | Specifies the working directory that contains all user configuration and working files for all OpenText SAST applications and Java IDE plugins. To configure this property, you must have write access to the directory.<br>**Defaults:**<br>• Windows—`${win32.LocalAppdata}/Fortify`<br>• Non-Windows—`${user.home}/.fortify`<br>**Tools Affected: AWB, ECP, CRE, IAP** |

# 1.5.3. Configuration Options for Fortify Extension for Visual Studio

This section describes the properties Fortify Extension for Visual Studio uses . The properties are listed in alphabetical order based on the files in which they belong.

# 1.5.3.1. Fortify Extension for Visual Studio Properties

Some properties described here already exist in the `fortify.properties` file, and some of them you must add yourself. The following table describes the properties in the *<tools_install_dir>*`/Core/config/fortify.properties` file.

| Property | Details |
|---|---|
| com.fortify.audit.ui.DisableBugtrackers | If set to `true`, disables bug tracker integration.<br>**Default:** `false` |
| com.fortify.audit.ui.DisableSuppress | If set to `true`, disables issue suppression.<br>**Default:** `false` |
| com.fortify.AuthenticationKey | Specifies the directory used to store the encrypted Application Security authentication token.<br>**Default:** `${com.fortify.WorkingDirectory}/config/VS`*<vs_version>*`-`*<extension_version>* |
| com.fortify.Debug | If set to `true`, runs all OpenText SAST tools in debug mode.<br>**Default:** `false` |
| com.fortify.model.CustomDescriptionsHeader | Specifies the custom prefix for the description header. It prepends the text in the `Description/Recommendation` header, so that you see "My Recommendations" instead of "Custom Recommendations."<br>**Note**<br>To update description headers, OpenText recommends that you use the `<CustomDescriptionRule>` rule with the `<Header>` element text instead.<br>**Default:** none |
| com.fortify.model.ForceIIDMigration | If set to `true`, forces running Instance ID migration during a merge.<br>**Default:** `false` |
| com.fortify.model.PriorityImpactThreshold | Specifies the threshold for issue impact. The valid values are 0.0F–5.0F. If the impact of an issue is greater than or equal to the threshold, the issue is considered High. If the impact of an issue is less than the threshold, the issue is considered Low. Issues are then categorized as follows:<br>• **Critical**—High Impact and High Likelihood<br>• **High**—High Impact and Low Likelihood<br>• **Medium**—Low Impact and High Likelihood<br>• **Low**—Low Impact and Low Likelihood<br>Also see com.fortify.model.PriorityLikelihoodThreshold<br>**Default:** `2.5F` |
| com.fortify.model.PriorityLikelihoodThreshold | Specifies the threshold for issue likelihood. The valid values are 0.0F–5.0F. If the likelihood of an issue is greater than or equal to the threshold, the issue is considered High. If the likelihood of an issue is less than the threshold, the issue is considered Low. Issues are then categorized as follows:<br>• **Critical**—High Impact and High Likelihood<br>• **High**—High Impact and Low Likelihood<br>• **Medium**—Low Impact and High Likelihood<br>• **Low**—Low Impact and Low Likelihood<br>Also see com.fortify.model.PriorityImpactThreshold<br>**Default:** 2.5F |

| | |
|---|---|
| com.fortify.<br>model.UseIIDMigrationFile | Specifies the full path of the instance ID migration file to use.<br>**Default:** none |
| com.fortify.<br>SCAExecutablePath | Specifies file path to `sourceanalyzer.exe`. |
| com.fortify.<br>search.defaultSyntaxVer | Specifies whether to use the AND and OR operators in searches. These are enabled in search syntax by default.<br>• To block the use of the AND and OR operators, set the value to `1`.<br>• To use ANDs and ORs without parentheses, set the value to `2`.<br>**Default:** `2` |
| com.fortify.<br>tools.iidmigrator.scheme | Set this property to migrate instance IDs created with different versions of OpenText SAST using a custom matching scheme. This is handled by OpenText SAST. If you need a custom matching scheme, contact Customer Support.<br>**Default:** none |
| com.fortify.<br>visualstudio.vm.args | Specifies JVM options.<br>**Default:** `-Xmx256m` |
| com.fortify.<br>VS.Debug | If set to `true`, runs the Fortify Extension for Visual Studio in debug mode.<br>**Default:** `false` |
| com.fortify.<br>VS.DisableCIntegration | If set to `true`, disables C/C++ build integration in Visual Studio.<br>**Default:** `false` |
| com.fortify.<br>VS.disableMigrationCheck | If set to `true`, disables instance ID migration checking.<br>**Default:** `false` |
| com.fortify.<br>VS.DisableReferenceLibDirs<br>AndExcludes | If set to `true`, disables using references added to a project.<br>**Default:** `false` |
| com.fortify.<br>VS.ListProjectProperties | If set to `true`, lists the Visual Studio project properties in a log file.<br>**Default:** `false` |
| com.fortify.<br>VS.NETFrameworkRoot | Specifies the file path to the .NET Framework root.<br>**Default:** none |
| com.fortify.<br>WorkingDirectory | Specifies the working directory that contains all user configuration and working files for Fortify Extension for Visual Studio. To configure this property, you must have write access to the directory.<br>**Default:** `${win32.LocalAppdata}/Fortify` |

# 1.5.3.2. Azure DevOps Server Configuration Property

The property for the Azure DevOps Server is stored in the `TFSconfiguration.properties`. This file is located in the Fortify working directory in the `config\VS<vs_version>-<sca_version>` directory.

**Note**

The `TFSconfiguration.properties` file is created only after the first time you configure a connection to your Azure DevOps Server from the Fortify Extension for Visual Studio.

The following property is in the `TFSconfiguration.properies` file:

`server.url`

**Details:** Specifies the Azure DevOps Server location.

**Default:** none

# 1.5.4. Shared Configuration Options

This section describes the properties shared by OpenText SAST applications and command-line tools.

# 1.5.4.1. Server Properties

Because some values in this file are encrypted (such as proxy user name and password), you must use the scapostinstall tool to configure these properties. For information about how to use the scapostinstall tool, see the *OpenText™ Static Application Security Testing User Guide*.

Other properties are updated using command-line tools, and standalone applications (such as Fortify Audit Workbench). OpenText recommends that you use these tools to edit the properties in this file instead of editing the file manually.

The following table describes the properties in the `<tools_install_dir>/Core/config/server.properties` file.

**Note**

After you specify the location of the OpenText SAST executable from Fortify Audit Workbench or Fortify Extension for Visual Studio, the location of the properties file changes to `/Core/config`.

| Property | Details |
|---|---|
| autoupgrade.server | Specifies the automatic update server. This enables users to check for new versions of the OpenText SAST and the OpenText™ Application Security Tools installer on a Application Security server and run the installer if an update is available.<br>**Default:** `http://localhost:8180/ssc/update-site/installers` |
| install.auto.upgrade | If set to `true`, enables Fortify Audit Workbench automatic update feature.<br>**Default:** `false` |
| oneproxy.http.proxy.port | Specifies the proxy server port to access bug trackers.<br>**Default:** none |
| oneproxy.http.proxy.server | Specifies the proxy server name to access bug trackers.<br>**Default:** none |
| oneproxy.https.proxy.port | Specifies the proxy server port to access bug trackers through an SSL connection.<br>**Default:** none |
| oneproxy.https.proxy.server | Specifies the proxy server name to access bug trackers through an SSL connection.<br>**Default:** none |
| rp.update.from.manager | If set to `true`, updates security content from Application Security instead of from the Fortify Rulepack update server.<br>**Default:** `false` |
| rulepack.auto.update | If set to `true`, updates security content automatically.<br>**Default:** `false` |
| rulepack.days | Specifies the interval (in days) between security content updates.<br>**Default:** `15` |
| rulepackupdate.proxy.port | Specifies the proxy server port to access the Fortify Rulepack update server (`uploadclient.proxy.port` is used if `rp.update.from.manager` is set to `true`).<br>Also see rp.update.from.manager<br>**Default:** none |
| rulepackupdate.proxy.server | Specifies proxy server name to access the Fortify Rulepack update server (`uploadclient.proxy.server` is used if `rp.update.from.manager` is set to `true`).<br>Also see rp.update.from.manager<br>**Default:** none |

| | |
|---|---|
| rulepackupdate.server | Specifies the Fortify Rulepack update server location.<br>**Default:** `https://update.fortify.com` |
| rulepackupdate.SocketReadTimeoutSeconds | Specifies the socket read timeout value to use when updating Fortify security content with the fortifyupdate utility.<br>**Default:** 180 seconds |
| uploadclient.proxy.port | Specifies the proxy server port to access the Application Security server.<br>**Default:** none |
| uploadclient.proxy.server | Specifies the proxy server name to access the Application Security server.<br>**Default:** none |
| uploadclient.server | Specifies the URL of the Application Security server.<br>**Default:** `http://localhost:8180/ssc` |

# 1.5.4.2. Command-Line Tools Properties

The following table describes the properties in the `<tools_install_dir>/Core/config/fortify.properties` file that the command-line tools use.

| Property | Details |
|---|---|
| com.fortify.log.console | Specifies whether logging messages are written to the console. Logging information is always written to the log file.<br>**Default:** `false` |

opentext™