Micro Focus
Fortify Static Code Analyzer

Software Version: 23.1.0

Applications and Tools Guide

Document Release Date: May 2023
Software Release Date: May 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

This document was produced on May 08, 2023. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

Contents

Preface

Contacting Micro Focus Fortify Customer Support

Visit the Support website to:

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

https://www.microfocus.com/support

For More Information

For more information about Fortify software products:

https://www.microfocus.com/cyberres/application-security

About the Documentation Set

The Fortify Software documentation set contains installation, user, and deployment guides for all Fortify Software products and components. In addition, you will find technical notes and release notes that describe new features, known issues, and last-minute updates. You can access the latest versions of these documents from the following Micro Focus Product Documentation website:

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

To be notified of documentation updates between releases, subscribe to Fortify Product Announcements on the Micro Focus Community:

https://community.microfocus.com/cyberres/fortify/w/fortify-product-announcements

Fortify Product Feature Videos

You can find videos that highlight Fortify products and features on the Fortify Unplugged YouTube channel:

https://www.youtube.com/c/FortifyUnplugged

About Fortify Static Code Analyzer Applications and Tools

The Fortify Applications and Tools installation includes applications and Fortify Secure Code Plugins that enable you to scan your code with Micro Focus Fortify Static Code Analyzer 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 Micro Focus Fortify Software Security Center.

The following table describes the Fortify Static Code Analyzer applications and tools that you can install with the Fortify Applications and Tools installer.

Application / Tool	Description	More Information
Fortify Audit Workbench	Provides a graphical user interface for Fortify Static Code Analyzer analysis results that helps you organize, investigate, and prioritize analysis results so that developers can fix security flaws quickly.	*Fortify Audit Workbench User Guide* in Fortify Static Code Analyzer and Tools Documentation
Fortify Plugin for Eclipse	Adds the ability to run Fortify Static Code Analyzer scans (either locally or remotely using Fortify 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.	*Fortify Plugin for Eclipse User Guide* in Fortify Static Code Analyzer and Tools Documentation
Fortify Analysis Plugin for IntelliJ IDEA and Android Studio	Adds the ability to run Fortify Static Code Analyzer scans (either locally or remotely using Fortify ScanCentral SAST) on the entire codebase of a project from IntelliJ IDEA and Android Studio. To view the analysis results, upload them to Fortify Software Security Center or open them in Fortify Audit Workbench.	*Fortify Analysis Plugin for IntelliJ IDEA and Android Studio User Guide* in Fortify Static Code Analyzer and Tools Documentation

Application / Tool	Description	More Information
Fortify Extension for Visual Studio	Adds the ability to run Fortify Static Code Analyzer scan (either locally or remotely using Fortify 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 Fortify Software Security Center server.	*Fortify Extension for Visual Studio User Guide* in Fortify Static Code Analyzer and Tools Documentation
Fortify Scan Wizard	Provides a graphical user interface that enables you to prepare a script to scan your code with Fortify Static Code Analyzer (either locally or remotely using Fortify ScanCentral SAST) and then optionally upload the results to Fortify Software Security Center.	"Fortify Scan Wizard" on page 19
Fortify Custom Rules Editor	Provides a graphical user interface to create and edit custom rules.	
BIRTReportGenerator ReportGenerator	Command-line tool to generate BIRT reports and legacy reports based on a Fortify Project Results (FPR) file.	"Generating Analysis Reports from the Command Line" on page 22

FPRUtility	Command-line tool that enables you to:
	• Merge audited projects
	• Verify FPR signatures
	• Display information from an FPR file including:
	  • Any errors associated with the analysis
	  • Number of issues
	  • Filtered lists of issues in different formats
	  • Lines of code for analyzed files
	  • List of analyzed functions
		"Working with FPR Files from the Command Line" on page 27

Application / Tool	Description	More Information
	• Mappings for a migrated project • Combine or split source code files and audit projects into FPR files • Alter an FPR	
fortifyclient	Command-line tool to create Fortify Software Security Center authentication tokens and securely transfer objects to and from Fortify Software Security Center. **Note:** Two versions of fortifyclient are included with the Fortify Applications and Tools installation: • SOAP API-based client in *<tools_install_dir>*/bin (this will be replaced by the REST API-based client in a future release) • REST API-based client in *<tools_install_dir>*/tools	*Fortify Software Security Center User Guide* in Fortify Software Security Center Documentation

The following table describes a tool that is included in the Fortify Static Code Analyzer Applications and Tools download package.

Tool	Description	More Information
Fortify Security Assistant Plugin for Eclipse	Provides alerts to potential security issues as you write your Java code. The alerts give you detailed information about security risks and recommendations for how to secure the potential issue.	*Fortify Security Assistant Plugin for Eclipse User Guide* in Fortify Security Assistant Plugin for Eclipse Documentation

Related Documents

This topic describes documents that provide information about Micro Focus Fortify software products.

Note: You can find the Fortify Product Documentation at https://www.microfocus.com/support/documentation. Most guides are available in both PDF and HTML formats. Product help is available within the Fortify LIM product.

All Products

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

Document / File Name	Description
About Fortify Product Software Documentation About_Fortify_Docs_<*version*>.pdf	This paper provides information about how to access Fortify product documentation. **Note:** This document is included only with the product download.
Fortify License and Infrastructure Manager Installation and Usage Guide LIM_Guide_<*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.
Fortify Software System Requirements Fortify_Sys_Reqs_<*version*>.pdf	This document provides the details about the environments and products supported for this version of Fortify Software.
Fortify Software Release Notes FortifySW_RN_<*version*>.pdf	This document provides an overview of the changes made to Fortify Software for this release and important information not included elsewhere in the product documentation.
What's New in Fortify Software <version> Fortify_Whats_New_<*version*>.pdf	This document describes the new features in Fortify Software products.

Fortify ScanCentral SAST

The following document provides information about Fortify ScanCentral SAST. Unless otherwise noted, this document is available on the Micro Focus Product Documentation website at https://www.microfocus.com/documentation/fortify-software-security-center.

Document / File Name	Description
Fortify ScanCentral SAST Installation, Configuration, and Usage Guide SC_SAST_Guide_<*version*>.pdf	This document provides information about how to install, configure, and use Fortify ScanCentral SAST to streamline the static code analysis process. It is written for anyone who intends to install, configure, or use Fortify ScanCentral SAST to offload the resource-intensive translation and scanning phases of their Fortify Static Code Analyzer process.

Fortify Software Security Center

The following document provides information about Fortify Software Security Center. Unless otherwise noted, this document is available on the Micro Focus Product Documentation website at https://www.microfocus.com/documentation/fortify-software-security-center.

Document / File Name	Description
Fortify Software Security Center User Guide SSC_Guide_<*version*>.pdf	This document provides Fortify Software Security Center users with detailed information about how to deploy and use Software Security Center. It provides all of the information you need to acquire, install, configure, and use Software Security Center. It is intended for use by system and instance administrators, database administrators (DBAs), enterprise security leads, development team managers, and developers. Software Security Center provides security team leads with a high-level overview of the history and current status of a project.

Fortify Static Code Analyzer

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

Document / File Name	Description
Fortify Static Code Analyzer User Guide SCA_Guide_<*version*>.pdf	This document describes how to install and use Fortify Static Code Analyzer to scan code on many of the major programming platforms. It is intended for people responsible for security audits and secure coding.
Fortify Static Code Analyzer Applications and Tools Guide SCA_Apps_Tools_<*version*>.pdf	This document describes how to install Fortify Static Code Analyzer applications and tools. It provides an overview of the applications and command-line tools that enable you to scan your code with Fortify Static Code Analyzer, review analysis results, work with analysis results files, and more.
Fortify Static Code Analyzer Custom Rules Guide SCA_Cust_Rules_Guide_<*version*>.zip	This document provides the information that you need to create custom rules for Fortify Static Code Analyzer. This guide includes examples that apply rule-writing concepts to real-world security issues. **Note:** This document is included only with the product download.
Fortify Audit Workbench User Guide AWB_Guide_<*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.
Fortify Plugin for Eclipse User Guide Eclipse_Plugin_Guide_<*version*>.pdf	This document provides information about how to install and use the Fortify Complete Plugin for Eclipse.
Fortify Analysis Plugin for IntelliJ IDEA and Android Studio User Guide IntelliJ_AnalysisPlugin_Guide_<*version*>.pdf	This document describes how to install and use Fortify Analysis Plugin for IntelliJ IDEA and Android Studio.

Document / File Name	Description
Fortify Extension for Visual Studio User Guide VS_Ext_Guide_<*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.
Fortify Static Code Analyzer Applications and Tools Properties Reference Guide SCA_Tools_Props_Ref_<*version*>.pdf	This document describes the properties used by Fortify Static Code Analyzer applications and command-line tools.

About Installing Fortify Static Code Analyzer Applications and Tools

This section describes how to install Fortify Static Code Analyzer applications and tools. See the *Fortify Software System Requirements* document to be 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 Fortify Static Code Analyzer Applications and Tools" on page 6.

You must provide a Fortify license file for the Fortify Static Code Analyzer Applications and Tools installation. The following table lists the different methods of installation.

Installation Method	Instructions
Perform the installation using a standard install wizard	"Installing Fortify Static Code Analyzer Applications and Tools" on the next page
Perform the installation silently (unattended)	"Installing Fortify Applications and Tools Silently (Unattended)" on page 14
Perform a text-based installation on non-Windows systems	"Installing Fortify Applications and Tools in Text-Based Mode on Non-Windows Platforms" on page 15

Installing Fortify Static Code Analyzer Applications and Tools

To install Fortify Static Code Analyzer applications and tools:

1. Run the installer file for your operating system to start the Fortify Applications and Tools Setup Wizard:
   - Windows: `Fortify_Apps_and_Tools_<version>_windows_x64.exe`
   - Linux: `Fortify_Apps_and_Tools_<version>_linux_x64.run`
   - macOS: `Fortify_Apps_and_Tools_<version>_osx_x64.app.zip`
     Uncompress the ZIP file before you run the APP installer file.

   where *<version>* is the software release version.
2. Click **Next**.
3. Review and accept the license agreement, and then click **Next**.
4. Choose where to install Fortify Applications and Tools, and then click **Next**.

   Important! Do not install Fortify Applications and Tools in the same directory where Fortify Static Code Analyzer is installed.
5. (Optional) Select the components to install, and then click **Next**.
6. Specify the path to the `fortify.license` file, and then click **Next**.
7. Specify if you want to migrate from a previous installation of Fortify Applications and Tools on your system.

   Migrating from a previous Fortify Applications and Tools installation preserves Fortify Applications and Tools artifact files. For more information, see "About Upgrading Fortify Static Code Analyzer Applications and Tools" on page 17.

   To migrate artifacts from a previous installation:
   a. In the Applications and Tools Migration page, select **Yes**, and then click **Next**.
   b. Specify the location of the existing Fortify Applications and Tools 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**.
8. If you are installing the Fortify Extension for Visual Studio, do the following:
   a. 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.
   b. Click **Next**.
9. Click **Next** on the Ready to Install page to install Fortify Applications and Tools.
10. Click **Finish** to close the Fortify Applications and Tools Setup Wizard.

Installing Fortify Applications and 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 Fortify Applications and Tools in the same directory where Fortify Static Code Analyzer is installed.

To install Fortify Applications and Tools silently:

1. Create an options file.
   a. 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.
   b. 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, 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 Audit Workbench, installation of Fortify Extension for Visual Studio 2022 for all users, and the target Fortify Applications and Tools installation directory:

      ```
      fortify_license_path=C:\Users\admin\Desktop\fortify.license
      MigrateTools=1
      enable-components=AWB_group,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, and the command-line tools, and the target Fortify Applications and Tools installation directory:

```
fortify_license_path=/opt/Fortify/fortify.license
MigrateTools=1
enable-components=AWB_group,Eclipse,CLI
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	`Fortify_Apps_and_Tools_<version>_windows_x64.exe --mode unattended --optionfile <full_path_to_options_file>`
Linux	`./Fortify_Apps_and_Tools_<version>_linux_x64.run --mode unattended --optionfile <full_path_to_options_file>`
macOS	You must uncompress the ZIP file before you run the command. `Fortify_Apps_and_Tools_<version>_osx_x64.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\FortifyAppsAndTools-<version>-install.log`
Linux **macOS**	`/tmp/FortifyAppsAndTools-<version>-install.log`

Installing Fortify Applications and 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 Fortify Applications and Tools in the same directory where Fortify Static Code Analyzer is installed.

To perform a text-based installation of Fortify Applications and Tools, run the text-based install command for your operating system as listed in the following table.

Linux	`./Fortify_Apps_and_Tools_<version>_linux_x64.run --mode text`
macOS	You must uncompress the provided ZIP file before you run the command. `Fortify_Apps_and_Tools_<version>_osx_x64.app/Contents/MacOS/installbuilder.sh --mode text`

Adding Trusted Certificates

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

- The Fortify Static Code Analyzer 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 Fortify Software Security Center. By default, these tools do not trust self- or locally-signed certificates.
- Fortify Static Code Analyzer configured as a Fortify ScanCentral SAST sensor uses an HTTPS connection to communicate with the Controller.

When using HTTPS, Fortify Static Code Analyzer 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 Fortify Static Code Analyzer applications and tools need to trust connections where the server presents a certificate issued by this CA, you must configure the Fortify Static Code Analyzer 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 Fortify Applications and Tools keystore. The Fortify Applications and 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 Fortify Applications and 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**.

About Upgrading Fortify Static Code Analyzer Applications and Tools

To upgrade Fortify Applications and 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 Fortify Applications and Tools artifact files located in the *<tools_install_dir>*`/Core/config` directory.

If you choose not to migrate any settings from a previous release, Fortify 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 Fortify Applications and Tools" on the next page.

Upgrading the Fortify Extension for Visual Studio

If you have administrative privileges and are upgrading from a previous version of the Fortify Applications and 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.

About Uninstalling Fortify Applications and Tools

This section describes how to uninstall Fortify Static Code Analyzer and Applications. 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.

Uninstalling Fortify Applications and Tools

To uninstall Fortify Applications and Tools:

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

Windows	`Uninstall_FortifyAppsAndTools_<version>.exe` Alternatively, you can do the following: a. Select **Start > Settings > Apps > Apps & Features**. b. From the list of programs, select **Fortify Applications and Tools <version>**, and then click **Uninstall**.
Linux	`Uninstall_FortifyAppsAndTools_<version>`
macOS	`Uninstall_FortifyAppsAndTools_<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 Fortify Applications and Tools that you are uninstalling.
   - Click **No** to retain the application settings on your system.

Uninstalling Fortify Applications and Tools Silently

To uninstall Fortify Applications and Tools silently:

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

Windows	`Uninstall_FortifyAppsAndTools_<version>.exe --mode unattended`
Linux	`./Uninstall_FortifyAppsAndTools_<version> --mode unattended`

macOS	`Uninstall_FortifyAppsAndTools_<version>.app/Contents/MacOS/installbuilder.sh --mode unattended`

Note: The uninstaller removes the application setting folders for the applications installed with the version of Fortify Applications and Tools that you are uninstalling.

Uninstalling Fortify Applications and Tools in Text-Based Mode on Non-Windows Platforms

To uninstall Fortify Applications and 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:

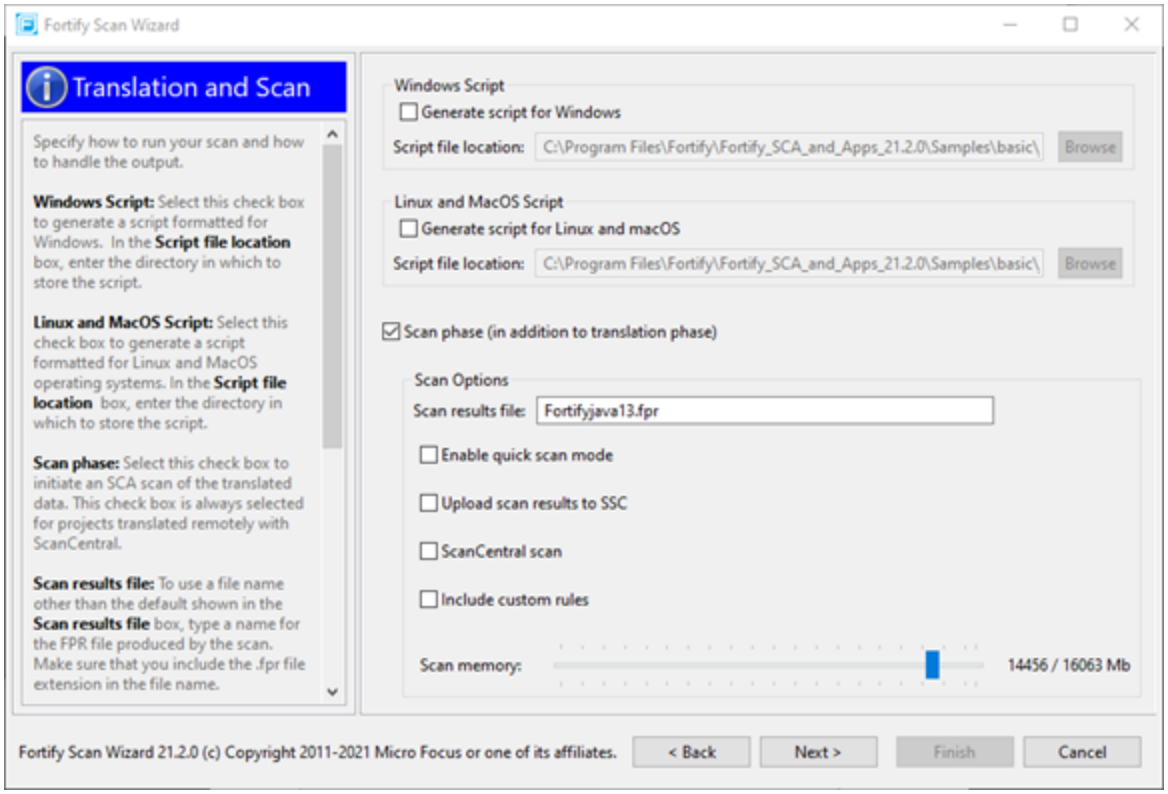
Linux	`./Uninstall_FortifyAppsAndTools_<version> --mode text`
macOS	`Uninstall_FortifyAppsAndTools_<version>.app/Contents/MacOS/installbuilder.sh --mode text`

Fortify Scan Wizard

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

Preparing to use Fortify Scan Wizard

Fortify Scan Wizard uses the information you provide to create a script with the commands for Micro Focus Fortify Static Code Analyzer to scan project code and optionally upload the analysis results to Micro Focus Fortify Software Security Center. You can use Fortify Scan Wizard to create a script that runs your scans locally or sends them to Micro Focus Fortify 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 Fortify Software Security Center.

Important! If Fortify Software Security Center or the Fortify 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 Fortify Static Code Analyzer (see the *Fortify Static Code Analyzer User Guide*).

Task	Requirements
Perform a local analysis with Fortify Static Code Analyzer	• Fortify Static Code Analyzer installed on the system where the generated script will be run. You can generate the script on a different platform without Fortify Static Code Analyzer, and then transfer the script to the system where it will be run.
Perform a remote analysis (translation and scan phases) with Fortify ScanCentral SAST	• Either a Fortify ScanCentral SAST client installed with the Fortify Static Code Analyzer installation or a standalone Fortify ScanCentral SAST client installation (see the *Fortify ScanCentral SAST Installation, Configuration, and Usage Guide* for instructions)

Task	Requirements
	• A Fortify ScanCentral SAST Controller URL **Note:** If you are also uploading analysis results to Fortify Software Security Center, then you do not need to specify a Controller URL. The Fortify ScanCentral SAST that is integrated with the Fortify Software Security Center server is used in this case. • Your project must be in a language that Fortify ScanCentral SAST supports for translation. See the *Fortify Software System Requirements* for a list of supported languages.
Perform a local Fortify Static Code Analyzer translation and a remote scan with Fortify ScanCentral SAST	• A Fortify ScanCentral SAST client installed with the Fortify Static Code Analyzer installation • A Fortify ScanCentral SAST Controller URL
Upload analysis results to Fortify Software Security Center	• A Fortify Software Security Center server URL **Note:** If you are using Fortify ScanCentral SAST, the Fortify Software Security Center server must be integrated with the Fortify ScanCentral SAST Controller. • Your Fortify Software Security Center login credentials **Note:** If you do not have Fortify Software Security Center login credentials, you must have an application name and version that exists in Fortify Software Security Center. • An authentication token of type ToolsConnectToken **Note:** If you do not have a token, you can use Fortify Scan Wizard to generate one. To do this, you must have Fortify Software Security Center 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.

Starting Fortify Scan Wizard

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

- On Windows, select **Start > All Programs > 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.

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 *Fortify Audit Workbench User Guide* for a description of the available report templates.

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" on the next page

"Troubleshooting BIRTReportGenerator" on page 25

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 ASVS 4.0"`, `"OWASP Mobile Top 10"`, `"OWASP Top 10"`, `"PCI DSS Compliance"`, and `"PCI SSF Compliance"`. **Note:** You only need to enclose the report template name in quotes if a space exists in the *<template_name>*. The template name values are ***not*** case-sensitive.
`-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. **Note:** The format values are ***not*** case-sensitive.
`-output <report_file.***>`	(Required) Specifies the file to which the report is written. **Note:** 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: `-searchQuery audited:false` For a description of the search query syntax, see the *Fortify Audit Workbench User Guide*.
`-ShowSuppressed`	Include issues that are marked as suppressed.

BIRTReportGenerator Option	Description
`-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 valid values for the template versions are listed below. The template version values are case-insensitive. **Note:** Templates that are not listed here have only one version available. 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. • For the "CWE Top 25" template, the version is `"CWE Top 25 <year>"` (for example, `"CWE Top 25 2022"`) • For the "CWE/SANS Top 25" template, the version is `"<year> CWE/SANS Top 25"` (for example, `"2011 CWE/SANS Top 25"`) • For the "DISA STIG" template, the version is `"DISA STIG <version>"` (for example, `"DISA STIG 5.2"`) • For the "FISMA Compliance" template, the version is `"NIST 800-53 Rev <version>"` (for example, `"NIST 800-53 Rev 5"`) • For the MISRA template, the available versions are `"MISRA C 2012"` or `"MISRA C++ 2008"` • For the "OWASP Top 10" template, the version is `"OWASP Top 10 <year>"` (for example, `"OWASP Top 10 2021"`)

BIRTReportGenerator Option	Description
	• For the "PCI DSS Compliance" template, the version is "PCI *<version>*" (for example, "PCI 4.0") **Note:** For versions earlier than 3.2.1, the version is "*<version>* Compliance" (for example, "3.2 Compliance") • 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.

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 myproject_report.pdf -Xmx32G
```

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 -showSuppressed -user Alex -f MyFortifyReport.pdf
```

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. **Note:** 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`. **Note:** Enclose the *<template_name>* in quotes if it contains any spaces. See the *Fortify Audit Workbench User Guide* for a description of the available report templates and how to customize them.

ReportGenerator Option	Description
`-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.

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 for an FPR File
- Extracting a Source Archive from an FPR File
- Altering FPR Files
- Allocating More Memory for FPRUtility

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 Fortify Software Security Center, *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. **Note:** 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 Fortify Static Code Analyzer and the Rulepack versions of the two projects are the same.

FPRUtility Option	Description
`-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: • `-i` provides a case-sensitive file name comparison of the merged files • `-u <scheme_file>` tells iidmigrator to read the matching scheme from `<scheme_file>` for instance ID migration **Note:** Wrap `<-iidmigrator_options>` in single quotes (`'-u <scheme_file>'`) when working from a Cygwin command prompt. Windows example: `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.

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 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.

FPRUtility Option	Description
`-information`	Displays information for the project.
Specify one of the following options to indicate what information to display:	
`-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 Fortify Static Code Analyzer and the Fortify 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. • Use `-search -queryAll` to search all the issues in the FPR including

FPRUtility Option	Description
	suppressed and removed issues. • 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:
	`<filename>: <total_loc> (<executable_loc>)`
	where *<total_loc>* is the approximate number of lines that contain code constructs (comments are excluded).
	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:
	• `+` indicates new analyzed files
	• `-` indicates removed analyzed files
	• `*` 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:
	`* ProjectA/main.jsp: 115 +15 (85 +7)`
	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 and 7 additional executable 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:
	`<sink_filename>:<line_num>` or
	`<sink_filename>:<line_num>` (`<category>` | `<analyzer>`)
	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>*).
	If you specify the `-outputFormat CSV` option, then each issue is displayed on one line in the format:
	`"<instanceid>", "<category>",`
	`"<sink_filename>:<line_num>", "<analyzer>"`

FPRUtility Option	Description
`-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. **Important!** 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.

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:
 	
`-extract`
`-mergeArchive`
`-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).

FPRUtility Option	Description
	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.

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. If you do not specify this option, then the merged FPR is altered.

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
```

Troubleshooting

By default, log files for Fortify Static Code Analyzer 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 Fortify Static Code Analyzer 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>`
BIRTReportGenerator	`BIRT-<version>`
fortifyclient	`FortifyClient-<version>`
FPRUtility	`FPRCommandlineInterface-<version>`
ReportGenerator	`ReportCommandlineInterface-<version>`

Samples

The Fortify Applications and Tools installation includes sample bug tracker plugins, an analysis results file that was scanned with Fortify Static Code Analyzer, and more.

The following table describes the samples in the *<tools_install_dir>*`/Samples` folder.

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

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email.

Note: If you are experiencing a technical issue with our product, do not email the documentation team. Instead, contact Micro Focus Fortify Customer Support at https://www.microfocus.com/support so they can assist you.

If an email client is configured on this computer, click the link above to contact the documentation team and an email window opens with the following information in the subject line:

Feedback on Applications and Tools Guide (Fortify Static Code Analyzer 23.1.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to fortifydocteam@microfocus.com.

We appreciate your feedback!