Micro Focus
Fortify Plugins for JetBrains IDEs and Android Studio

Software Version: 22.1.0

User Guide

Document Release Date: Revision 1: July 2022
Software Release Date: June 2022

MICRO FOCUS

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

All trademarks, service marks, product names, and logos included in this document are the property of their respective owners.

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 July 06, 2022. 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 5
Contacting Micro Focus Fortify Customer Support 5
For More Information 5
About the Documentation Set 5
Fortify Product Feature Videos 5

Change Log 6

Chapter 1: Introduction 8
About Fortify Plugins for JetBrains IDEs and Android Studio 8
Related Documents 9
All Products 9
Micro Focus Fortify ScanCentral SAST 10
Micro Focus Fortify Software Security Center 10
Micro Focus Fortify Static Code Analyzer 11

Chapter 2: Using the Fortify Analysis Plugin 12
About the Fortify Analysis Plugin Installation 12
Installing the Fortify Analysis Plugin 12
Uninstalling the Fortify Analysis Plugin 13
Fortify Security Content 13
Updating Fortify Security Content 14
Updating Fortify Security Content on a Network that uses a Proxy Server 14
About Analyzing the Source Code 15
About Scanning Locally 15
Setting Memory for Code Analysis 16
Setting the Query Language Type 16
Selecting the Fortify Security Content to Apply During Analysis 16
Using Quick Scan 17
Excluding Dependent Modules from Analysis 17
Specifying Additional Fortify Static Code Analyzer Options 18
Synchronizing with Fortify Software Security Center 19

Scanning Projects Locally 19
Performing an Advanced Local Scan 21
About Scanning with Fortify ScanCentral SAST 24
Configuring Fortify ScanCentral SAST Options 25
Scanning Projects with Fortify ScanCentral SAST 28
Performing an Advanced Scan with Fortify ScanCentral SAST 29
Uploading Analysis Results to Fortify Software Security Center 33
Locating Analysis Plugin Log Files 34

Chapter 3: Using the Fortify Remediation Plugin 36
About the Fortify Remediation Plugin Installation 36
Installing the Fortify Remediation Plugin 36
Uninstalling the Fortify Remediation Plugin 37
Opening Fortify Software Security Center Application Versions 37
Viewing Analysis Results 38
Viewing and Selecting Issues 39
Grouping Issues 41
Customizing Issue Visibility 43
Searching for Issues 44
Search Modifiers 45
Search Query Examples 50
Performing Searches 51
Viewing Issue Information 51
Audit Tab 51
Analysis Trace 52
Recommendations Tab 54
Details Tab 55
History Tab 55
Updating Audit Information 55
Assigning Users to Issues 56
Assigning Tags to Issues 56
Adding Comments to Issues 56
Locating Issues in your Source Code 57
Locating Remediation Plugin Log Files 57

Send Documentation Feedback 58

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

Change Log

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

Software Release / Document Version	Change
22.1.1 / Revision 1: July 2022	Updated: Fortify Remediation Plugin version 22.1.1 • "Opening Fortify Software Security Center Application Versions" on page 37 - New command to disconnect from Fortify Software Security Center • "Viewing and Selecting Issues" on page 39 - New pagination of issues in the Fortify Remediation window into subfolders when the number of issues exceeds the issue pagination setting • "Grouping Issues" on page 41 - Added grouping options available when you remediate analysis results on Micro Focus Fortify Software Security Center
22.1.0	Updated: • Minor edits
21.2.0	Updated: • "Configuring Fortify ScanCentral SAST Options" on page 25 - New ability to include test files in the scan
21.1.0	Added: • "About Analyzing the Source Code" on page 15, "About Scanning with Fortify ScanCentral SAST" on page 24, and "Performing an Advanced Scan with Fortify ScanCentral SAST" on page 29 - New ability to scan projects with Micro Focus Fortify ScanCentral SAST Removed: • Enabling Findbugs During Scans - Fortify Static Code Analyzer no longer supports this feature.

Software Release / Document Version	Change
20.2.0	Updated: • "Scanning Projects Locally" on page 19, "Uploading Analysis Results to Fortify Software Security Center" on page 33, and "Opening Fortify Software Security Center Application Versions" on page 37 - New ability to connect to Fortify Software Security Center with an authentication token • "Uploading Analysis Results to Fortify Software Security Center" on page 33 and "Opening Fortify Software Security Center Application Versions" on page 37 - New ability to connect to Fortify Software Security Center with an authentication token

Chapter 1: Introduction

This guide provides information about how to install and use:

- The Micro Focus Fortify Analysis Plugin to scan your code from IntelliJ IDEA or Android Studio with Micro Focus Fortify Static Code Analyzer
- The Micro Focus Fortify Remediation Plugin to review issues on a Micro Focus Fortify Software Security Center server from JetBrains IDEs and Android Studio.

This section contains the following topics:

About Fortify Plugins for JetBrains IDEs and Android Studio 8

Related Documents 9

About Fortify Plugins for JetBrains IDEs and Android Studio

The Fortify Analysis Plugin works in the IntelliJ IDEA and the Android Studio integrated development environment (IDE). The Fortify Remediation Plugin works in the IntelliJ IDEA, Android Studio, PyCharm, and WebStorm IDEs. Developers use these plugins to:

- Scan a codebase for vulnerabilities with either a local installation of Micro Focus Fortify Static Code Analyzer or remotely with Micro Focus Fortify ScanCentral SAST
- Integrate with Micro Focus Fortify Software Security Center
- Review the analysis results to eliminate false positives and prioritize the order of remediation
- Fix and eliminate security vulnerabilities in your code (remediation)

You can install the plugin that best fits your needs or install both plugins.

To do this	Use this plugin
Initiate a scan from the IDE to generate analysis results	Fortify Analysis Plugin
Upload analysis results to Fortify Software Security Center	
Integrate with Fortify Software Security Center to review the analysis results	Fortify Remediation Plugin
Review analysis results, assign users or tags to issues, and add comments to issues	

Related Documents

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

Note: You can find the Micro Focus 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 Micro Focus Fortify Product Software Documentation About_Fortify_Docs_<*version*>.pdf	This paper provides information about how to access Micro Focus Fortify product documentation. **Note:** This document is included only with the product download.
Micro Focus 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.
Micro Focus 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.
Micro Focus 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 Micro Focus Fortify Software <version> Fortify_Whats_New_<*version*>.pdf	This document describes the new features in Fortify Software products.

Micro Focus Fortify ScanCentral SAST

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

Document / File Name	Description
Micro Focus 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.

Micro Focus Fortify Software Security Center

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

Document / File Name	Description
Micro Focus 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.

Micro Focus 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
Micro Focus 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.
Micro Focus 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.

Chapter 2: Using the Fortify Analysis Plugin

The Fortify Analysis Plugin focuses on scanning your project to identify vulnerabilities quickly and easily in the code. You can use the Fortify Analysis Plugin with IntelliJ IDEA and Android Studio.

After you install the Fortify Analysis Plugin, you can configure your analysis options and then scan your project with Micro Focus Fortify Static Code Analyzer. Your organization can use the analysis results with Micro Focus Fortify Software Security Center to manage projects and assign issues to the relevant developers.

This chapter describes how to install the Fortify Analysis Plugin, use it to uncover vulnerabilities in your source code, and upload the analysis results to Fortify Software Security Center.

This section contains the following topics:

About the Fortify Analysis Plugin Installation 12
Fortify Security Content 13
About Analyzing the Source Code 15
About Scanning Locally 15
About Scanning with Fortify ScanCentral SAST 24
Uploading Analysis Results to Fortify Software Security Center 33
Locating Analysis Plugin Log Files 34

About the Fortify Analysis Plugin Installation

You can install the Fortify Analysis Plugin on Windows, Linux, and macOS. For information about which operating system versions are supported, see the *Micro Focus Fortify Software System Requirements* document.

Installing the Fortify Analysis Plugin

Note: These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.

To install the Fortify Analysis Plugin:

1. Run the Micro Focus Fortify Static Code Analyzer and Applications installation and select IntelliJ IDEA Analysis from the list of plugins.
2. Start IntelliJ IDEA or Android Studio.

3. Open the Settings dialog box as follows:
   - On Windows or Linux, select **File > Settings**.
   - On macOS, select ***<IDE_name>*** **> Preferences**.
4. On the left, select **Plugins**.
5. Select **Install Plugin from Disk**, browse to the `<sca_install_dir>/plugins/IntelliJAnalysis` directory, and then select `Fortify_IntelliJ_Analysis_Plugin_<version>.zip`.
6. Click **OK**.
7. To activate the plugin, restart the IDE.

The menu bar now includes the **Fortify** menu.

Uninstalling the Fortify Analysis Plugin

Note: These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.

To uninstall the Fortify Analysis Plugin:

1. Start IntelliJ IDEA or Android Studio.
2. Open the Settings dialog box as follows:
   - On Windows or Linux, select **File > Settings**.
   - On macOS, select ***<IDE_name>*** **> Preferences**.
3. On the left, select **Plugins**.
4. From the installed **Plugins** list, select **Fortify Analysis**.
5. Select **Uninstall**.

Fortify Security Content

Micro Focus Fortify Static Code Analyzer uses a knowledge base of rules to enforce secure coding standards applicable to the codebase for static analysis. Fortify Security Content (security content) consists of Secure Coding Rulepacks and external metadata:

- Secure Coding Rulepacks describe general secure coding idioms for popular languages and public APIs
- External metadata includes mappings from the Fortify categories to alternative categories (such as CWE, OWASP Top 10, and PCI)

Fortify provides the ability to write custom rules that add to the functionality of Fortify Static Code Analyzer and the Secure Coding Rulepacks. For example, you might need to enforce proprietary

security guidelines or analyze a project that uses third-party libraries or other pre-compiled binaries that are not already covered by the Secure Coding Rulepacks. You can also customize the external metadata to map Fortify issues to different taxonomies, such as internal application security standards or additional compliance obligations. For instructions on how to create your own custom rules or custom external metadata, see the *Micro Focus Fortify Static Code Analyzer Custom Rules Guide*.

You must have security content on your local system to perform a scan locally or if you use Fortify ScanCentral SAST and run the translation locally (see "About Analyzing the Source Code" on the next page). Fortify strongly recommends that you periodically update the security content.

Updating Fortify Security Content

To update the security content:

1. Open a command prompt, and then navigate to the `<sca_install_dir>/bin` directory.
2. Do one of the following:
   - To download and update security content from the Rulepack update server, type `fortifyupdate`.
     If your network uses a proxy server to reach the Rulepack update server, see "Updating Fortify Security Content on a Network that uses a Proxy Server" below.
   - To update the security content from a local ZIP file that contains archived security content, type `fortifyupdate -import <zip_file>`.

Updating Fortify Security Content on a Network that uses a Proxy Server

If your network uses a proxy server to reach the Rulepack update server, you must use the scapostinstall utility to specify the proxy server.

To specify a proxy for the Rulepack update server and download the latest security content:

1. Open a command window, and then navigate to the `<sca_install_dir>/bin` directory.
2. At the command prompt, type `scapostinstall`.
3. Type `2` to select `Settings`.
4. Type `2` to select `Fortify Update`.
5. Type `2` to select `Proxy Server`, and then type the name of the proxy server.
6. Type `3` to select `Proxy Server Port`, and then type the proxy server port number.
7. (Optional) You can also specify the proxy server user name (option `4`) and password (option `5`).
8. Type `q` to close scapostinstall.
9. At the command prompt, type `fortifyupdate`.

About Analyzing the Source Code

A security analysis with Micro Focus Fortify Static Code Analyzer includes the following phases:

- Translate the source code into intermediate files
- Scan the intermediate files to complete the security analysis

There are two ways to analyze your source code:

- Use the locally installed and licensed Fortify Static Code Analyzer to perform the entire analysis (translation and scan phases). For information about how to configure and run the analysis locally, see "About Scanning Locally" below.

  To view the analysis results, upload the analysis results to a Micro Focus Fortify Software Security Center server by doing either of the following:

  - Automatically upload your changes each time you scan your project (see "Synchronizing with Fortify Software Security Center" on page 19).
  - Manually upload the analysis results (see "Uploading Analysis Results to Fortify Software Security Center" on page 33).

  Note: You can also open the analysis results (FPR) file in Fortify Audit Workbench

- Use Micro Focus Fortify ScanCentral SAST to perform the entire analysis (translation and scan phases) or only the scan phase. For information about how to configure and run the analysis using Fortify ScanCentral SAST, see "About Scanning with Fortify ScanCentral SAST" on page 24

  Note: If you use Fortify ScanCentral SAST to perform only the scan phase, then the Fortify Analysis Plugin performs the translation phase using the locally installed Fortify Static Code Analyzer.

  To view the analysis results, configure the Fortify Analysis Plugin to upload the analysis results to a Fortify Software Security Center server. Alternatively, you can use the provided job token in the Fortify ScanCentral SAST command-line interface to retrieve the analysis results (FPR) file (see the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*). You can then open the analysis results file in Fortify Audit Workbench.

After you upload the analysis results to Fortify Software Security Center, you can use the Fortify Remediation Plugin to view them in IntelliJ or Android Studio (see "Using the Fortify Remediation Plugin" on page 36).

About Scanning Locally

This section describes how to perform a scan of your source code on the local system. In the analysis configuration, you can specify how much memory to use during the scans, the SQL type, select the security content you want to use, whether you want to scan in quick scan mode, and other advanced

scanning options. You can also configure synchronizing the analysis results with Micro Focus Fortify Software Security Center.

Fortify strongly recommends that you periodically update the security content, which contains Secure Coding Rulepacks and external metadata. For information about how to update the security content, see "Updating Fortify Security Content" on page 14.

Setting Memory for Code Analysis

If you plan to analyze large projects, and you want to make sure you do not run out of memory during analysis, consider increasing the amount of memory that Micro Focus Fortify Static Code Analyzer uses for scanning.

To specify the amount of memory that Fortify Static Code Analyzer uses to scan a project:

1. Select **Fortify > Analysis Settings**.
   The Fortify Analysis Settings dialog box opens to the **Analysis Configuration** tab.
2. Under **Scan Configuration**, in the **Memory (MB)** box, type an integer.
   If no other memory-intensive processes are running, Fortify recommends that you allocate no more than two thirds of the available physical memory.

   Note: The Fortify Analysis Plugin warns you if you specify more memory than is physically available to applications on your system.
3. Click **OK**.

Setting the Query Language Type

By default, the Fortify Analysis Plugin treats SQL files as though they use the T-SQL procedural language on Windows systems and PL/SQL on other platforms. (Micro Focus Fortify Static Code Analyzer determines the SQL type setting by the `com.fortify.sca.fileextensions.sql` property in the `fortify-sca.properties` file.)

To set the procedural language for analysis:

1. Select **Fortify > Analysis Settings**.
   The Fortify Analysis Settings dialog box opens to the **Analysis Configuration** tab.
2. Under **Scan Configuration**, from the **SQL type** list, select **TSQL** or **PLSQL**.
3. Click **OK**.

Selecting the Fortify Security Content to Apply During Analysis

By default, the Fortify Analysis Plugin uses all available security content to analyze projects. You can narrow the focus of what the Fortify Analysis Plugin looks for during a scan by selecting the security content that it uses to analyze your project.

To specify the security content used to analyze a project:

1. Select **Fortify > Analysis Settings**.
   The Fortify Analysis Settings dialog box opens to the **Analysis Configuration** tab.
2. Under **Security Content**, clear the **Use all installed security content** check box.
3. In the **Installed Fortify Security Content** list, select the check boxes for the rules to apply during the scan.
4. If you have custom security content installed, in the **Installed Custom Security Content** list, select the check boxes for the custom security content you want to apply during the scan.
5. Click **OK**.

Using Quick Scan

Quick scan mode provides a way to quickly scan your projects for critical- and high-priority issues. Fortify Static Code Analyzer performs the scan faster by reducing the depth of the analysis and applying the Quick View filter set. Quick scan settings are configurable. For more details about the configuration of quick scan mode, see the *Micro Focus Fortify Static Code Analyzer User Guide*.

Quick scans are a great way to get many applications through an assessment so that you can quickly find issues and begin remediation. The performance improvement you get depends on the complexity and size of the application. Although the scan is faster than a full scan, it does not provide as robust a result set. Other issues that a quick scan cannot detect might exist in your application. Fortify recommends that you run full scans whenever possible.

Note: By default, Fortify Software Security Center does not permit you to upload scans performed in quick scan mode. However, you can configure your Fortify Software Security Center application version so that uploaded audit projects scanned in quick scan mode are processed. For more information, see analysis results processing rules in the *Micro Focus Fortify Software Security Center User Guide*.

To enable quick scan mode:

1. Select **Fortify > Analysis Settings**.
2. Select the **Advanced Options** tab.
3. Select the **Enable quick scan mode** check box.
4. Click **OK**.

Excluding Dependent Modules from Analysis

By default, the Fortify Analysis Plugin includes all source files from dependent modules in scans. Although you can scan individual modules, analysis results are more accurate if you scan an entire project together.

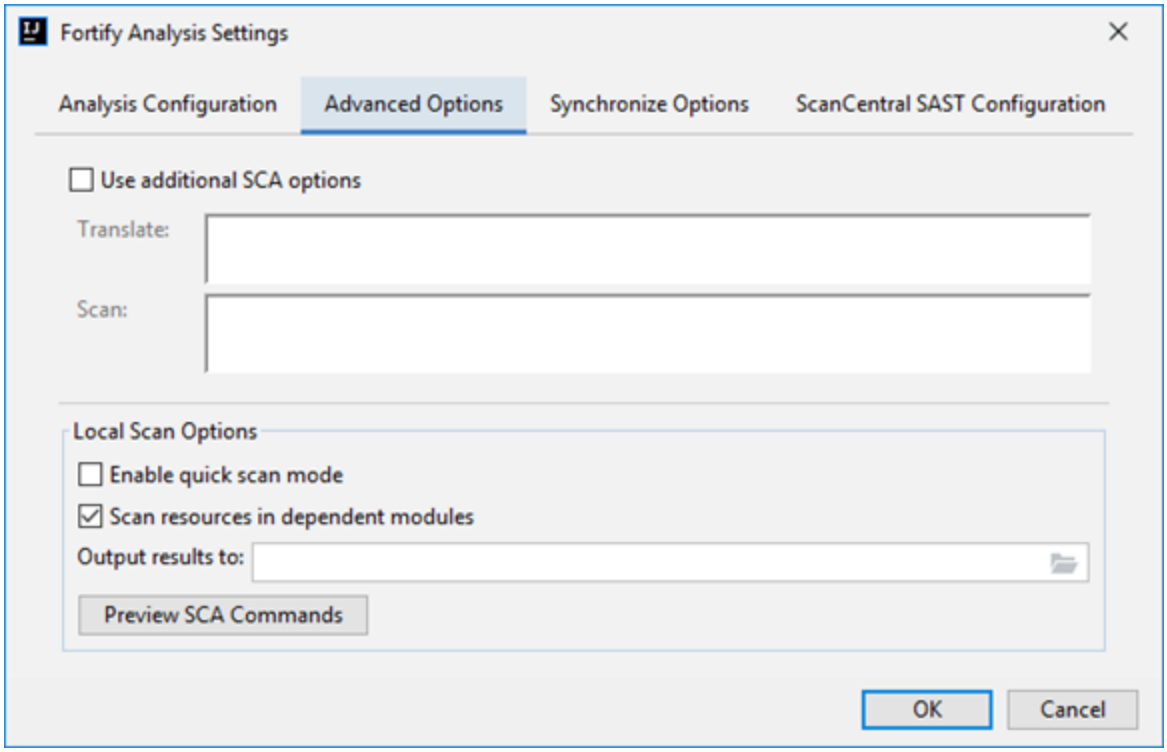
To exclude dependent or nested modules from analysis:

1. Select **Fortify > Analysis Settings**.
2. Select the **Advanced Options** tab.
3. Clear the **Scan resources in dependent modules** check box.
4. Click **OK**.

Specifying Additional Fortify Static Code Analyzer Options

To specify additional Micro Focus Fortify Static Code Analyzer options:

1. Select **Fortify > Analysis Settings**.
2. Select the **Advanced Options** tab.



3. Select the **Use additional SCA options** check box.
4. In the **Translate** and **Scan** boxes, type command-line options for the translation and scan phases, respectively.

   For example, if you include the `-verbose` command-line option, the Fortify Analysis Plugin sends detailed status messages to the console during the analysis. For information about the available command-line options and syntax, see the *Micro Focus Fortify Static Code Analyzer User Guide*.
5. To change the output location for your analysis results, click **Browse** to the right of the **Output results to** box, and then, in the Select output directory dialog box, specify the directory in which to save the results.

   By default, the analysis results are saved in the source project folder.

6. (Optional) Click **Preview SCA Commands** to see the Fortify Static Code Analyzer command-line options to be used in the analysis.
7. Click **OK**.

Synchronizing with Fortify Software Security Center

You can automatically upload your changes to an application version on Micro Focus Fortify Software Security Center each time you scan your local project. This synchronization helps facilitate collaborative auditing and enables you to synchronize any source code changes each time you rescan the project.

Note: Automatic synchronization requires that you specify an application version that already exists in Fortify Software Security Center. If the application version does not exist in Fortify Software Security Center, you must first create it. For instructions, see the *Micro Focus Fortify Software Security Center User Guide*.

To enable synchronization with Fortify Software Security Center:

1. Select **Fortify > Analysis Settings**.
2. Select the **Synchronize Options** tab.
3. In the **Server URL** box, specify the URL for your Fortify Software Security Center server.
4. If required, specify a proxy server and port number.
5. Select the **Synchronize project with server** check box.
6. Click **OK**.

Scanning Projects Locally

This topic describes how to use the Fortify Analysis Plugin to analyze your Java source code using the locally installed Micro Focus Fortify Static Code Analyzer to uncover security vulnerabilities.

Note: Fortify strongly recommends that you periodically update the security content, which contains Rulepacks and external metadata. For information about how to update security content, see "Updating Fortify Security Content" on page 14.

Note: If your project is an Android Gradle project, build the release target for the project so that the final project artifacts are generated before the scan. Doing this provides more accurate analysis results. You can either build the release target manually, before you start the scan, or later, as described in the following procedure.

To scan a project on the local system:

1. Do one of the following:
   - Select **Fortify > Analyze Project**.
   - Right-click a module, and then select **Analyze Module**.

Note: If your project is an Android Gradle project, the plugin prompts you to build the release target for the project so that the final project artifacts are generated. In the Rebuild the release target dialog box, click **Yes**.

2. If prompted, specify the path to the Fortify Static Code Analyzer executable, and then click **OK**.

   The Fortify Static Code Analyzer scan starts. The progress bar at the bottom of the window displays the progress of events during the scan. After the scan is completed, the Fortify Analysis Plugin saves the resulting Fortify Project Results (FPR) file. By default, the analysis results are saved in the source project folder. You can specify a different output location prior to a scan (see "Specifying Additional Fortify Static Code Analyzer Options" on page 18).

3. If your analysis settings are configured to synchronize with Micro Focus Fortify Software Security Center:

   a. If prompted to login to Fortify Software Security Center:

      i. If you have not already configured the URL for Fortify Software Security Center, type the server URL in the **SSC URL** box.

      ii. From the **Login method** menu, select the login method set up for you on Fortify Software Security Center.

      iii. Depending on the selected login method, follow the procedure described in the following table.

Login Method	Procedure
Username/Password	Type your Fortify Software Security Center user name and password.
Authentication Token	Specify the decoded value of a Fortify Software Security Center authentication token of type ToolsConnectToken. **Note:** For instructions about how to create an authentication token from Fortify Software Security Center, see the *Micro Focus Fortify Software Security Center User Guide*.

   b. Select the application version that corresponds to your IntelliJ or Android Studio project, and then click **OK**.

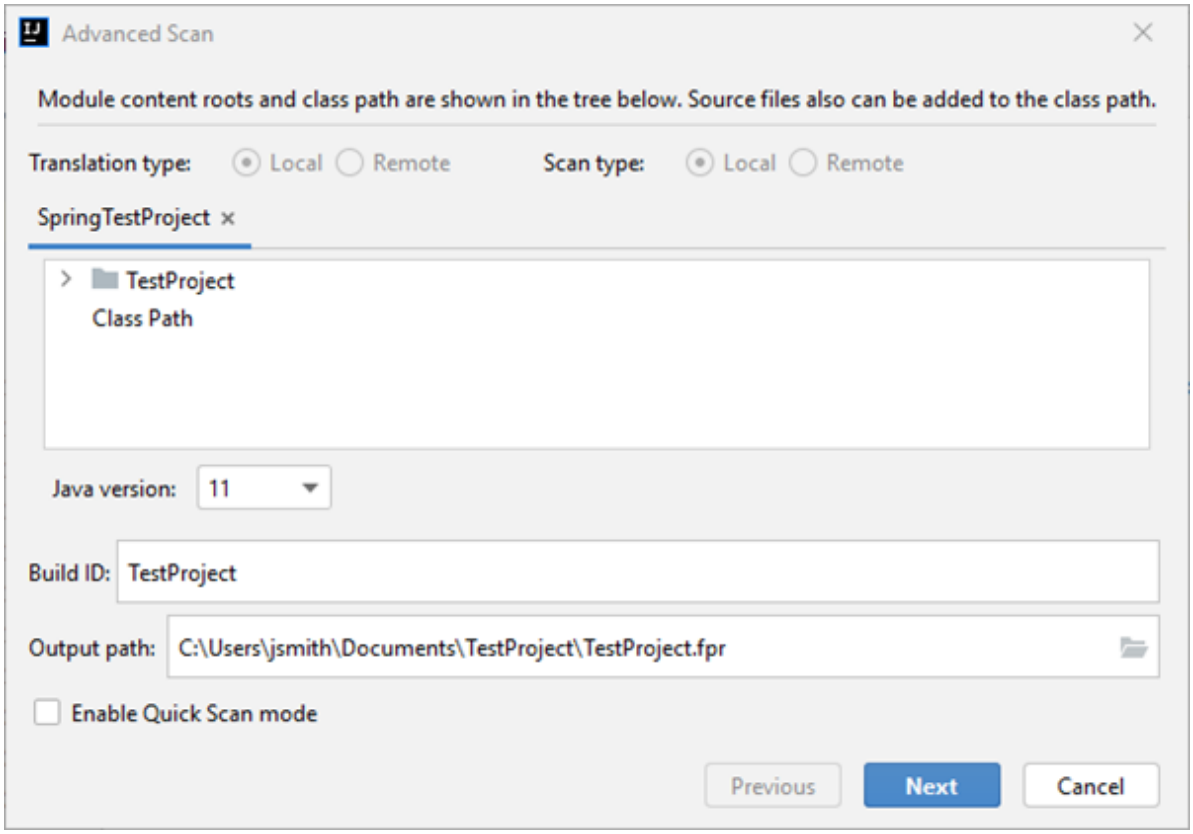
   If you have disabled synchronize project with Fortify Software Security Center, you can configure the connection later, and then upload the analysis results (see "Uploading Analysis Results to Fortify Software Security Center" on page 33).

Performing an Advanced Local Scan

Use the advanced scan to change the analysis options from those configured in the analysis settings and perform a local scan for a specific project. Use the advanced scan to translate and analyze Java projects that have source code in multiple directories, have special translation or build conditions, or have files that you want to exclude from the project.

To perform an advanced scan:

1. Select **Fortify > Advanced Scan**.
   The Advanced Scan wizard automatically includes all source files configured in the IDE.



   When you scan several modules, the wizard displays several tabs, one for each module. All modules are translated separately but analyzed together. If you want to exclude a module, close its tab.

   Note: The **Translation type** and **Scan type** options are unavailable when Fortify ScanCentral SAST upload is not enabled. To run an advanced scan with Fortify ScanCentral SAST, see "Performing an Advanced Scan with Fortify ScanCentral SAST" on page 29.

2. To exclude files or directories that contain, for example, test source code, right-click the file or directory, and then select **Exclude**.

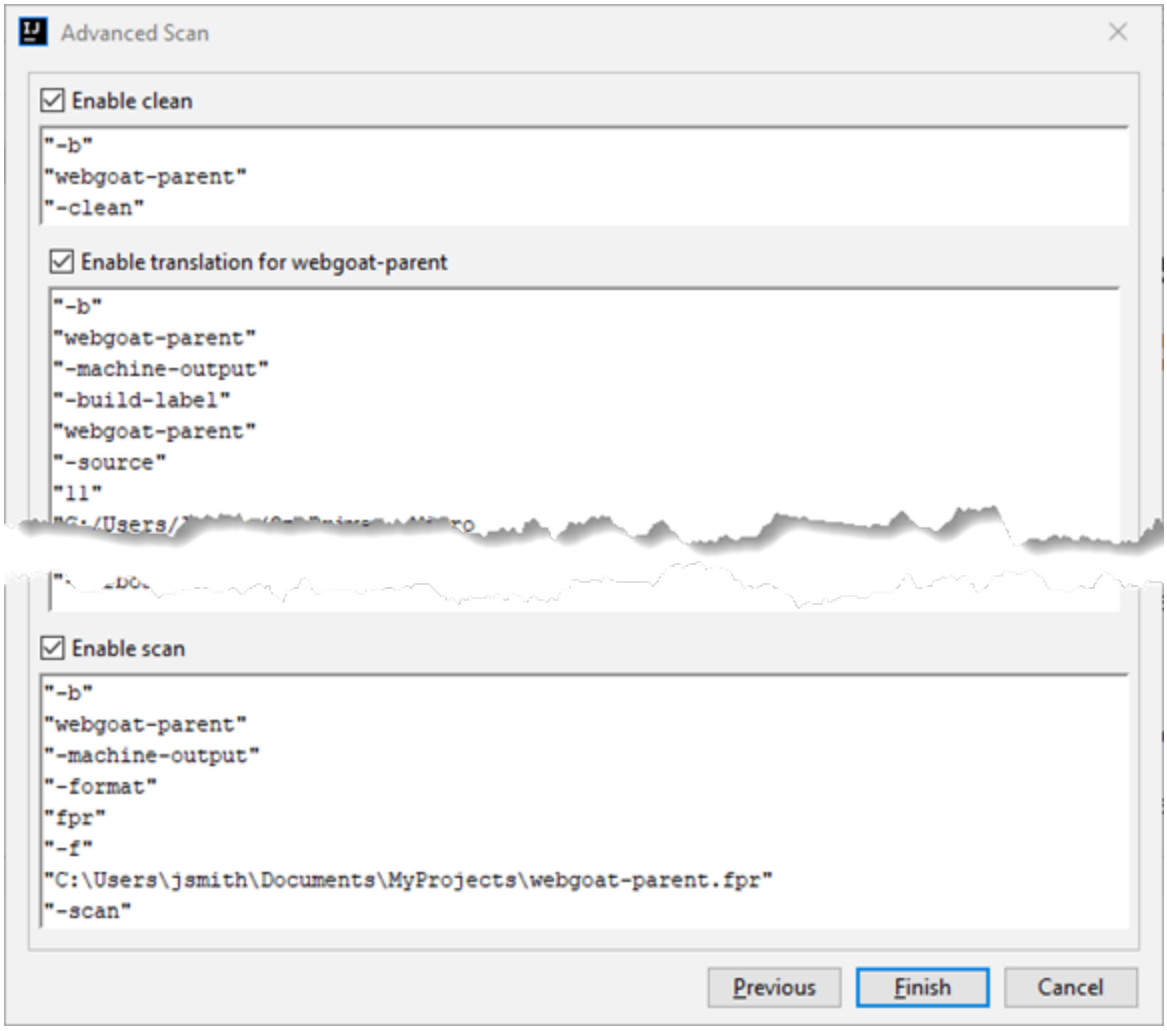
3. The Fortify Analysis Plugin automatically detects the class path from the IntelliJ or Android Studio project settings. To add folders that the plugin has not detected as in the class path, right-click a build directory, and then select **Add to ClassPath**.
4. From the **Java version** list, select the Java version for the project.
5. In the **Build ID** box, type the build ID.

   The project name is the default build ID with unacceptable file system symbols escaped.
6. To specify a different output file path than the default, in the **Output path** box, type the path and file name for the Fortify Project Results (FPR) file that Micro Focus Fortify Static Code Analyzer will generate.
7. To perform a quick scan, select the **Enable Quick Scan mode** check box.

   For information about quick scans, see "Using Quick Scan" on page 17.

8. Click **Next**.

   A preview of the Fortify Static Code Analyzer command-line options to be used in the analysis is displayed.



   The analysis process includes the following phases:

   - During the *clean* phase, Fortify Static Code Analyzer removes files from a previous translation of the project.
   - During the *translation* phase, you can see one translation section for each of the selected modules. You can modify the class path and all build parameters for each module separately. Fortify Static Code Analyzer translates source code identified in the previous screen into an intermediate format associated with the build ID. (The build ID is typically the project name.)
   - During the *scan* phase, Fortify Static Code Analyzer analyzes the source files identified during the translation phase and generates analysis results in the FPR format.

   Any additional Fortify Static Code Analyzer options configured on the **Advanced Options** tab in analysis settings are shown here. You can modify any of the Fortify Static Code Analyzer options.

For information about the available command-line options, see the *Micro Focus Fortify Static Code Analyzer User Guide*.

9. (Optional) To skip an analysis phase, clear the **Enable clean**, **Enable translation**, or **Enable scan** check box.

   For example, if the security content has changed but the project has not changed, you might want to disable the **translation** phase so that Fortify Static Code Analyzer scans the project without retranslating.
10. Click **Finish**.

About Scanning with Fortify ScanCentral SAST

This topic describes the requirements for using Micro Focus Fortify ScanCentral SAST to analyze your code and to upload the analysis results to Micro Focus Fortify Software Security Center. For instructions about how to configure the Fortify ScanCentral SAST options, see "Configuring Fortify ScanCentral SAST Options" on the next page.

With Fortify ScanCentral SAST, you can either:

- Perform the entire analysis (translation and scan) with Fortify ScanCentral SAST
- Perform the translation locally and then automatically upload the translated project to Fortify ScanCentral SAST for the scan phase

  You must translate the project or solution locally if it uses a language that Fortify ScanCentral SAST does not support for remote translation. For a list of supported languages, see the *Micro Focus Fortify Software System Requirements* document.

  You must have a locally installed and licensed Fortify Static Code Analyzer to perform the translation phase.

  Make sure that the Fortify Security Content version on the local system is the same as the version on the Fortify ScanCentral sensor. Fortify strongly recommends that you periodically update the security content. For information about how to update the security content locally, see "Updating Fortify Security Content" on page 14. Use the fortifyupdate utility to update security content on the ScanCentral sensor (see the *Micro Focus Fortify Static Code Analyzer User Guide*).

To analyze your code with Fortify ScanCentral SAST, you need the following:

- A properly configured Fortify ScanCentral SAST installation. For more information, see the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.
- To connect to Fortify ScanCentral SAST, you need either:
  - A ScanCentral Controller URL

    Important! If the ScanCentral Controller uses an SSL connection from an internal certificate authority or a self-signed certificate, you must import the certificate into the Java Keystore for Fortify Static Code Analyzer (in `<sca_install_dir>/jre/lib/security`) and for the IDE. For more information, see the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

- A Fortify Software Security Center URL and an authentication token of type ToolsConnectToken

  To configure the Fortify Software Security Center URL, see "Synchronizing with Fortify Software Security Center" on page 19.

  Important! If the Fortify Software Security Center uses an SSL connection from an internal certificate authority or a self-signed certificate, you must import the certificate into the Java Keystore for Fortify Static Code Analyzer (in `<sca_install_dir>/jre/lib/security`) and for the IDE. For more information, see the *Micro Focus Fortify Software Security Center User Guide*.

To send the analysis results to a Fortify Software Security Center server, you need the following:

- A Fortify Software Security Center URL or a ScanCentral Controller that is integrated with a Fortify Software Security Center server.

  Note: Fortify recommends that the Fortify Software Security Center URL configured in the analysis settings (Synchronize Options) is the same as the Fortify Software Security Center server integrated with the ScanCentral Controller.

- A Fortify Software Security Center authentication token of type ToolsConnectToken

  For instructions about how to create an authentication token, see the *Micro Focus Fortify Software Security Center User Guide*.
- An application version that exists in Fortify Software Security Center
- Permission to access the application and application version to which you want to upload

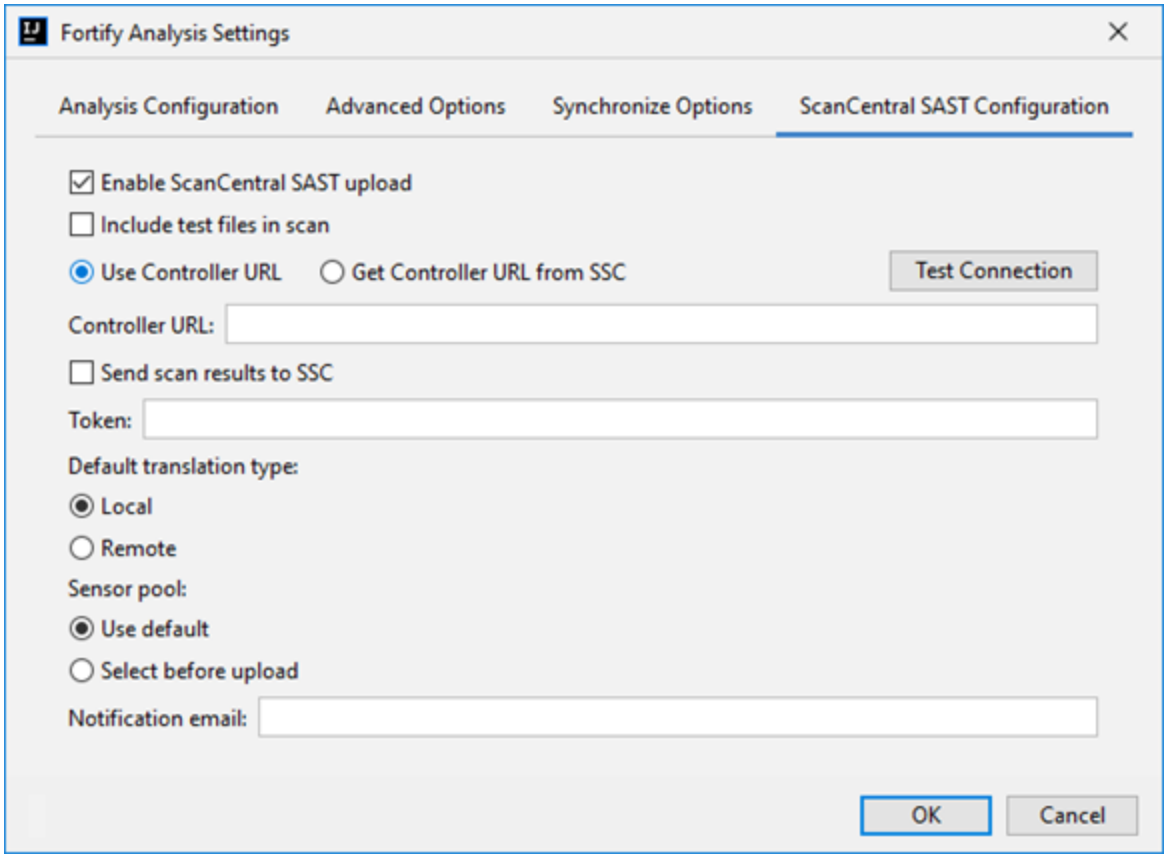
Configuring Fortify ScanCentral SAST Options

This topic describes how to configure the default Micro Focus Fortify ScanCentral SAST options to use when you submit a project for analysis. You can specify the translation type (local or remote), the Fortify Static Code Analyzer translation and scan options, the sensor pool selection, and whether to upload analysis results to Micro Focus Fortify Software Security Center.

To configure the Fortify ScanCentral SAST options:

1. Select **Fortify > Analysis Settings**.
2. Select the **ScanCentral SAST Configuration** tab.

3. Select **Enable ScanCentral SAST upload**.



4. (Optional) Select **Include test files in scan** to include the test source set (Gradle) or a test scope (Maven) with the scan.
5. To specify how to connect to Fortify ScanCentral SAST, do one of the following:
   - Select **Use Controller URL**, and then in the **Controller URL** box, type the URL for the ScanCentral Controller.

     Example: `https://<controller_host>:<port>/scancentral-ctrl`

     Tip: Click **Test Connection** to confirm that the URL is valid, and the Controller is accessible.
   - Select **Get Controller URL from SSC**, and then in the **Token** box, paste the decoded token value for an authentication token of type ToolsConnectToken.

     Note: For instructions about how to create an authentication token from Fortify Software Security Center, see the *Micro Focus Fortify Software Security Center User Guide*.

     Make sure you that have the Fortify Software Security Center URL that is integrated with the ScanCentral Controller provided on the **Synchronize Options** tab (see "Synchronizing with Fortify Software Security Center" on page 19).

Tip: Click **Test Connection** to confirm that the URL and token is valid, and the server is accessible.

6. To upload the analysis results to Fortify Software Security Center, select the **Send scan results to SSC** check box.
   - In the **Token** box, paste the decoded token value for an authentication token of type ToolsConnectToken.

     Note: If you connect to Fortify ScanCentral SAST using a Controller URL, analysis results are uploaded to the Fortify Software Security Center server specifically integrated with the ScanCentral Controller.
7. Under **Default translation type**, specify where to run the translation phase of the analysis by selecting one of the following:
   - **Local**—Run the translation phase on the local system and the scan phase with Fortify ScanCentral SAST.
   - **Remote**—Run the entire analysis with Fortify ScanCentral SAST.
8. Under **Sensor pool**, specify whether to use the default sensor pool or to be provided a list of sensor pools to choose from when you run a Fortify ScanCentral SAST scan.

   Note: If Fortify ScanCentral SAST is in SSC lockdown mode, the sensor pool selection is disabled. Fortify ScanCentral SAST automatically uses either the sensor pool associated with a selected application version or the default sensor pool.
9. (Optional) In the **Notification email** box, type an email address for job status notification.
10. (Optional) To specify Micro Focus Fortify Static Code Analyzer command-line options for the translation or scan phase:
    a. Select the **Advanced Options** tab.
    b. Select the **Use additional SCA options** check box and type Fortify Static Code Analyzer command-line options for the translation or scan phase.

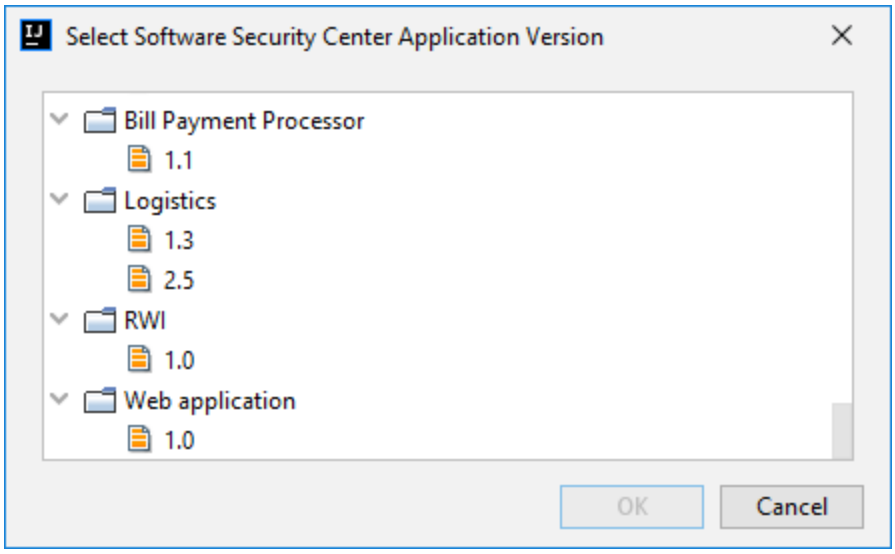
       For detailed information about the available Fortify Static Code Analyzer options and the proper syntax, see the *Micro Focus Fortify Static Code Analyzer User Guide*.
11. Click **OK** to save the configuration.

Scanning Projects with Fortify ScanCentral SAST

Before you can scan your project with Fortify ScanCentral SAST, you must configure the Fortify ScanCentral SAST options as described in "Configuring Fortify ScanCentral SAST Options" on page 25. If you want to override the default Fortify ScanCentral SAST options for a specific project, use the Advanced Scan wizard ("Performing an Advanced Scan with Fortify ScanCentral SAST" on the next page.

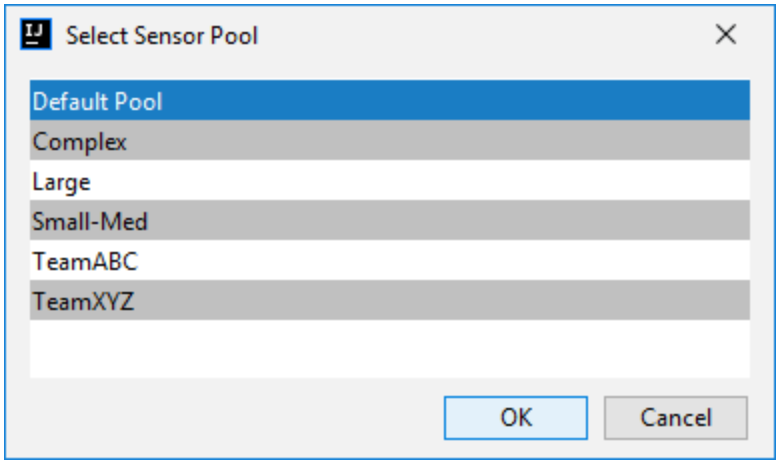
To scan a project with Fortify ScanCentral SAST:

1. Select **Fortify > Analyze Project with ScanCentral**.
2. If prompted, select the application version where you want to upload the analysis results, and then click **OK**.



3. If prompted, select a sensor pool from the Select Sensor Pool dialog box, and then click **OK**.

Note: The following Select Sensor Pool dialog box contains sample sensor pool names.



To view the analysis results, you can either:

- Copy the provided job token and use it in the Fortify ScanCentral SAST command-line interface to check the status and retrieve the analysis results (see the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*). You can then open the analysis results (FPR) file in Fortify Audit Workbench.

  Tip: If you need to retrieve the job token, you can find it in the Fortify ScanCentral SAST log file. The default log file locations are listed in "Locating Analysis Plugin Log Files" on page 34.

- If you uploaded the analysis results to Fortify Software Security Center, you can check the status of the job (and view the analysis results) on the Fortify Software Security Center server. After the scan is complete, you can use the Fortify Remediation Plugin to view the analysis results in IntelliJ or Android Studio (see "Using the Fortify Remediation Plugin" on page 36).

Performing an Advanced Scan with Fortify ScanCentral SAST

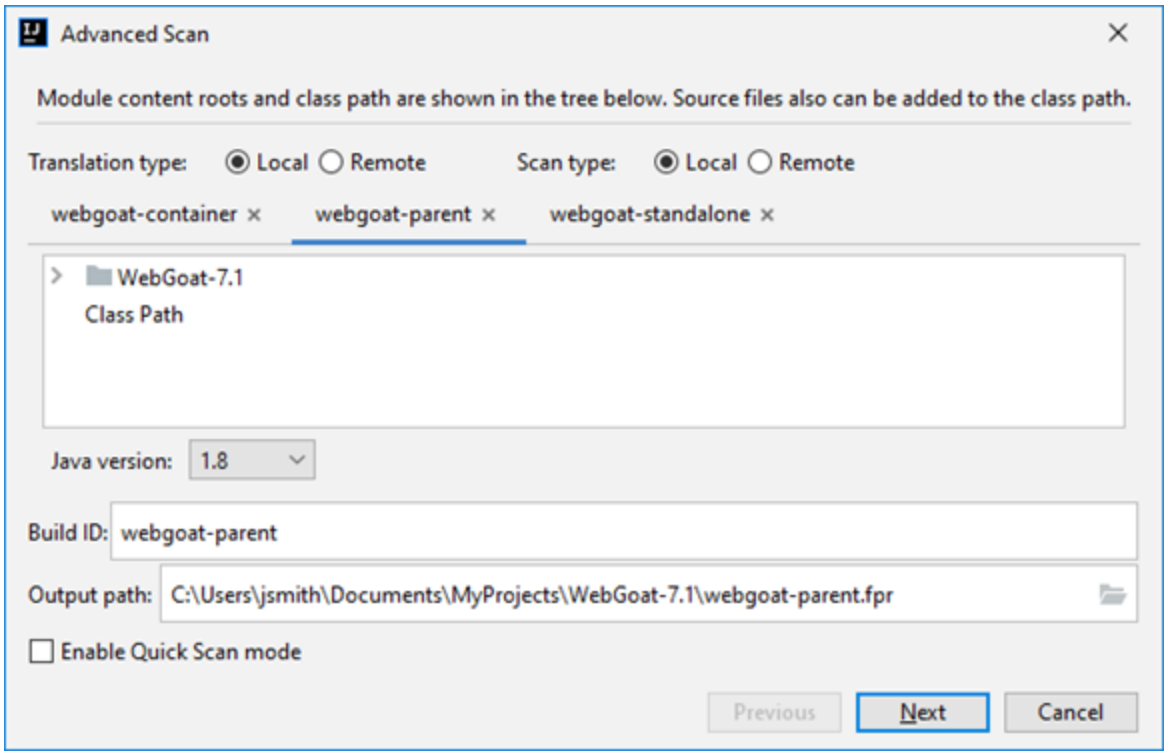
Use the Advanced Scan wizard to change the analysis options for a specific project from those configured in the analysis settings. Make sure that you have enabled Fortify ScanCentral SAST upload (see "Configuring Fortify ScanCentral SAST Options" on page 25).

Important! If you want to upload the analysis results to Fortify Software Security Center, make sure that you have specified an authentication token in the Fortify ScanCentral SAST configuration. For more information, see "Configuring Fortify ScanCentral SAST Options" on page 25.

To perform an advanced scan using Fortify ScanCentral SAST:

1. Select **Fortify > Advanced Scan**.

   The Advanced Scan wizard automatically includes all source files configured in IntelliJ or Android Studio.



When you scan several modules, the wizard displays a tab for each module. All modules are translated separately but analyzed together. To exclude a module, close its tab.

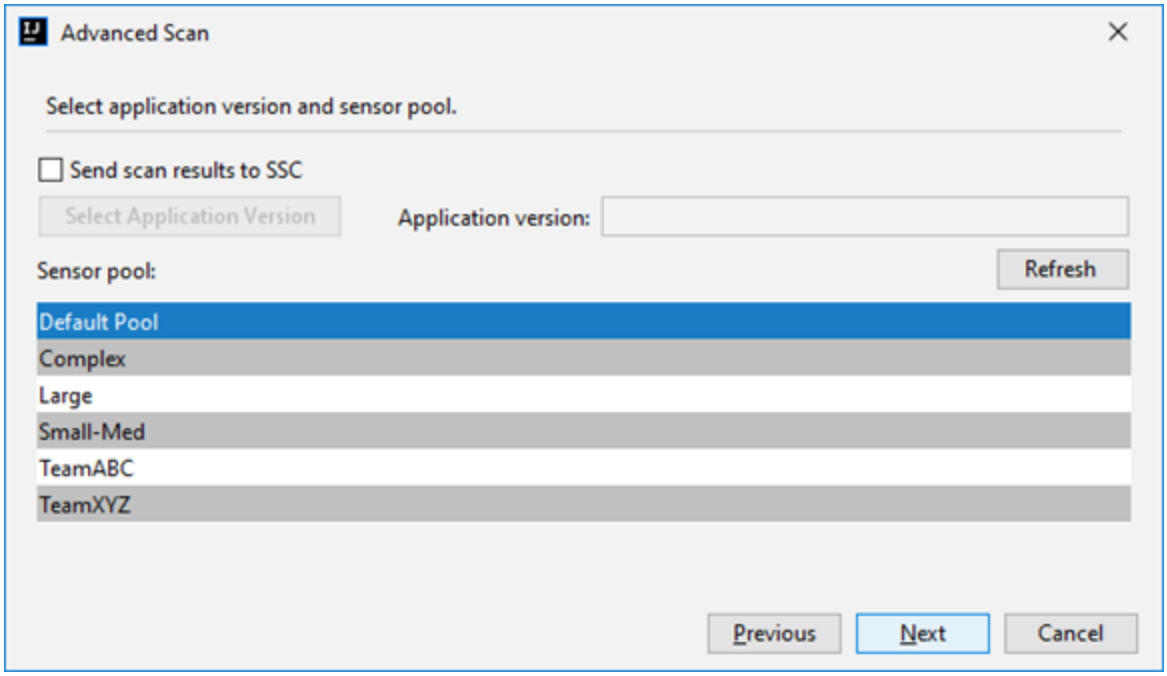
Note: The following options are only available for analysis performed entirely on a local system: **Java version**, **Build ID**, **Output path**, and **Enable Quick Scan mode**. You can ignore these options for analysis with Fortify ScanCentral SAST.

2. Specify where you want to run the translation and scan phases of the analysis by doing one of the following:
   - To run the translation phase on the local system and the scan phase with Fortify ScanCentral SAST, select **Local** for **Translation type** and **Remote** for **Scan type**.
   - To run the entire analysis with Fortify ScanCentral SAST, select **Remote** for **Translation type**.

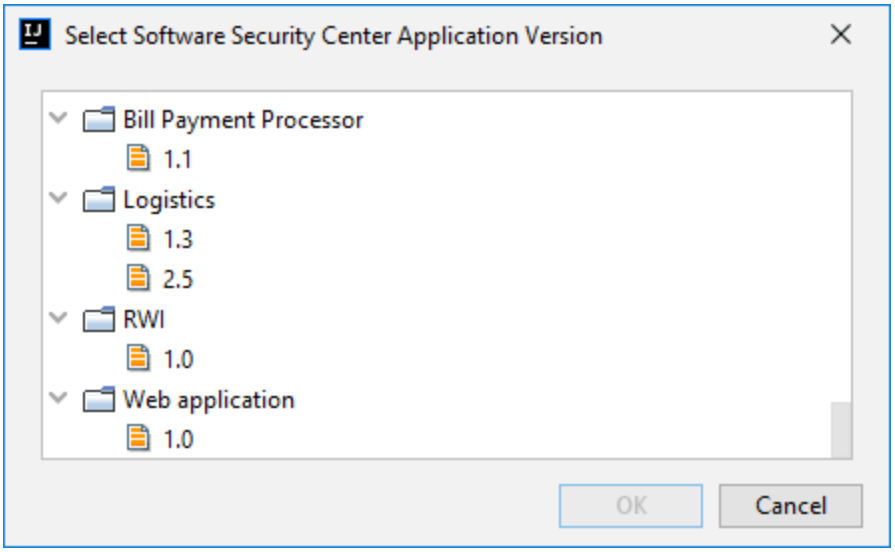
     Note: When you select **Remote** for the translation type, then **Scan type** is automatically set to **Remote**.
   - To run the entire analysis on the local system, select **Local** for both **Translation type** and **Scan type**. Skip the rest of this procedure and see "Performing an Advanced Local Scan" on page 21.

   Note: If both the **Translation type** options are disabled and you want to use Fortify ScanCentral SAST for any part of the analysis, you must first enable Fortify ScanCentral SAST upload (see "Configuring Fortify ScanCentral SAST Options" on page 25).
3. To exclude files or directories that contain, for example, test source code, right-click the file or directory, and then select **Exclude**.

4. The Fortify Analysis Plugin automatically detects the class path from the IntelliJ or Android Studio project settings. To add folders that the plugin has not detected in the class path, right-click a build directory and select **Add to ClassPath**.
5. Click **Next**.



6. To upload the analysis results to Fortify Software Security Center, select the **Send scan results to SSC** check box and do the following:
   a. Click **Select Application Version**.



   b. Select the application version where you want to upload the analysis results, and then click **OK**.

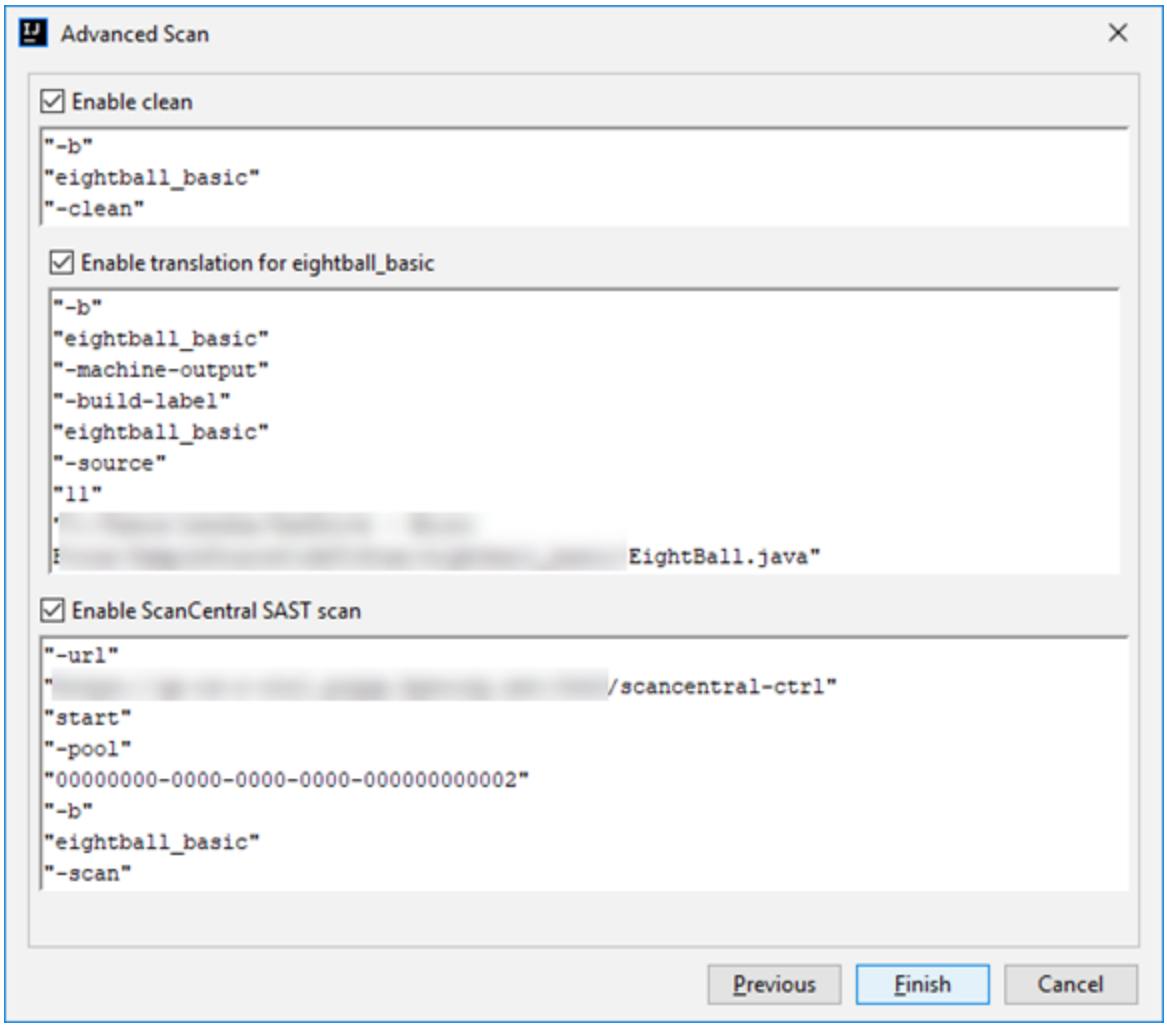
7. From the **Sensor pool** list, select a sensor pool.

   Note: If Fortify ScanCentral SAST is in SSC lockdown mode, the sensor pool selection is disabled. Fortify ScanCentral SAST automatically uses either the sensor pool associated with a selected application version or the default sensor pool.

8. Click **Next**.

   A preview of the Fortify Static Code Analyzer and Fortify ScanCentral SAST command-line options to be used in the analysis is displayed.

   The following image shows an example of a local translation and remote scan preview.



   The preview shows the commands-lines for the following phases:

   - (Local translation only) During the *clean* phase, Fortify Static Code Analyzer removes files from a previous translation of the project.

- (Local translation only) During the *translation* phase, you can see one translation section for each selected module. You can modify the class path and build parameters for each module individually. Fortify Static Code Analyzer translates source code identified in the previous screen into an intermediate format associated with the build ID. (The build ID is typically the project name.)

  Any additional Fortify Static Code Analyzer translation options configured on the **Advanced Options** tab in the analysis settings are shown here. You can modify any of the Fortify Static Code Analyzer options. For information about the available command-line options, see the *Micro Focus Fortify Static Code Analyzer User Guide*.

- The Fortify Analysis Plugin uses the Fortify ScanCentral SAST start command to start a remote scan. You cannot modify this command.

9. (Optional) To skip an analysis phase, clear the **Enable clean**, or **Enable translation for <proj_name>** check box.
10. Click **Finish**.

Uploading Analysis Results to Fortify Software Security Center

You can manually upload analysis results to Micro Focus Fortify Software Security Center any time after a local analysis is completed. However, before you do, a corresponding application version must already exist in Fortify Software Security Center.

Note: By default, Fortify Software Security Center does not permit you to upload scans performed in quick scan mode. However, you can configure your Fortify Software Security Center application version so that uploaded audit projects scanned in quick scan mode are processed. For more information, see analysis results processing rules in the *Micro Focus Fortify Software Security Center User Guide*.

To upload analysis results to Fortify Software Security Center:

1. Make sure that you have a generated FPR file in the default location (the source project folder) or the location configured in the analysis settings (see step 6 in "Specifying Additional Fortify Static Code Analyzer Options" on page 18).

   The FPR file must already exist.
2. From the IntelliJ or Android Studio menu bar, select **Fortify > Upload Results to Software Security Center**.

   The Software Security Center Credentials dialog box opens.
3. If prompted to login to Fortify Software Security Center:
   a. If you have not already configured the URL for Fortify Software Security Center, type the server URL in the **SSC URL** box.
   b. From the **Login method** menu, select the login method set up for you on Fortify Software Security Center.

c. Depending on the selected login method, follow the procedure described in the following table.

Login Method	Procedure
Username/Password	Type your Fortify Software Security Center user name and password.
Authentication Token	Specify the decoded value of a Fortify Software Security Center authentication token of type ToolsConnectToken. **Note:** For instructions about how to create an authentication token from Fortify Software Security Center, see the *Micro Focus Fortify Software Security Center User Guide*.

4. Select the Fortify Software Security Center application version that corresponds to your IntelliJ or Android Studio project, and then click **OK**.

You can now open the application and view the analysis results from Fortify Software Security Center or from the Fortify Remediation Plugin. For information about how to view and work with analysis results in Fortify Software Security Center, see the *Micro Focus Fortify Software Security Center User Guide*. For information about how to view and work with analysis results from IntelliJ or Android Studio, see "Using the Fortify Remediation Plugin" on page 36.

Locating Analysis Plugin Log Files

For help diagnosing a problem with the Analysis Plugin, provide the log files to Micro Focus Fortify Customer Support. The default locations for the log files are:

- On Windows:
  - C:\Users\<*username*>\AppData\Local\Fortify\sca<*version*>\log

    Log files in this directory are only created when you analyze the code locally with Micro Focus Fortify Static Code Analyzer.
  - C:\Users\<*username*>\AppData\Local\Fortify\IntelliJAnalysis-<*version*>\log
  - C:\Users\<*username*>\AppData\Local\Fortify\scancentral-<*version*>\log

    Log files in this directory are only created when you analyze the code with Micro Focus Fortify ScanCentral SAST.
- On Linux and macOS:
  - <*userhome*>/.fortify/sca<*version*>/log

    Log files in this directory are only created when you analyze the code locally with Fortify Static Code Analyzer.

- *<userhome>*/.fortify/IntelliJAnalysis-*<version>*/log
- *<userhome>*/.fortify/scancentral-*<version>*/log

  Log files in this directory are only created when you analyze the code with Fortify ScanCentral SAST.

Chapter 3: Using the Fortify Remediation Plugin

This chapter describes how to install the Fortify Remediation Plugin, use it to view analysis results stored on Micro Focus Fortify Software Security Center and assign specific issues to the relevant developers. You can use the Fortify Remediation Plugin with IntelliJ IDEA, Android Studio, PyCharm, and WebStorm.

This section contains the following topics:

About the Fortify Remediation Plugin Installation 36
Opening Fortify Software Security Center Application Versions 37
Viewing Analysis Results 38
Viewing Issue Information 51
Updating Audit Information 55
Locating Issues in your Source Code 57
Locating Remediation Plugin Log Files 57

About the Fortify Remediation Plugin Installation

You can install the Fortify Remediation Plugin on Windows, Linux, and macOS.

Note: You do not need to specify a Fortify license file for the Fortify Remediation Plugin. Only Micro Focus Fortify Software Security Center requires a license file.

Installing the Fortify Remediation Plugin

Note: These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.

To install the Fortify Remediation Plugin:

1. Open a project in the IDE.
2. Open the Settings dialog box as follows:
   - On Windows or Linux, select **File > Settings**.
   - On macOS, select ***<IDE_Name>*** **> Preferences**.
3. In the left pane, select **Plugins**.

4. Select **Install Plugin from Disk**, and then locate and select `Fortify_IntelliJ_Remediation_Plugin_<version>.zip`.
   For Information about where to acquire the installation file, see the *Micro Focus Fortify Software System Requirements* document.
5. Click **OK**.
6. To activate the plugin, restart the IDE.

The menu bar now includes the **Fortify** menu.

Uninstalling the Fortify Remediation Plugin

Note: These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.

To uninstall the Fortify Remediation Plugin:

1. Start the IDE.
2. Open the Settings dialog box as follows:
   - On Windows or Linux, select **File > Settings**.
   - On macOS, select ***<IDE_Name>* > Preferences**.
3. In the left pane, select **Plugins**.
4. From the **Plugins** list, select **Fortify Remediation**.
5. In the **Fortify Remediation** pane on the right, click **Uninstall**.
6. In the **Fortify Remediation** pane on the right, click **Restart**.

Opening Fortify Software Security Center Application Versions

To use the Fortify Remediation Plugin, you must first connect to Micro Focus Fortify Software Security Center.

Note: To use HTTPS to communicate with Fortify Software Security Center, you must import a trusted certificate for the IDE.

To open an application version in the Fortify Remediation Plugin:

1. Select **Fortify > Connect to Software Security Center**.
2. If prompted to login to Fortify Software Security Center:
   a. If you have not already configured the URL for Fortify Software Security Center, type the server URL in the **SSC URL** box.

b. From the **Login method** menu, select the login method set up for you on Fortify Software Security Center.
c. Depending on the selected login method, follow the procedure described in the following table.

Login Method	Procedure
Username/Password	Type your Fortify Software Security Center user name and password.
Authentication Token	Specify the decoded value of a Fortify Software Security Center authentication token of type ToolsConnectToken. **Note:** For instructions about how to create an authentication token from Fortify Software Security Center, see the *Micro Focus Fortify Software Security Center User Guide*.

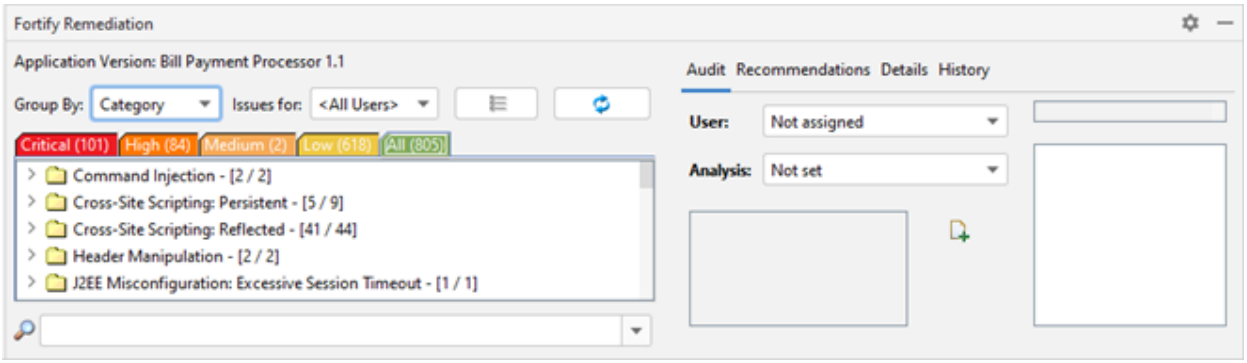
3. Select an application version to open, and then click **OK**.

The Fortify Remediation Plugin displays the analysis results for the application version from Fortify Software Security Center in the IDE.

Note: To open a different application version on the same Fortify Software Security Center server to which you are already connected, select **Fortify > Open Application Version**. To switch to a different Fortify Software Security Center server, select **Fortify > Disconnect from Software Security Center** and then reconnect to Fortify Software Security Center as described in this topic.

Viewing Analysis Results

The Fortify Remediation Plugin provides the analysis results for the opened application version. The Fortify Remediation window displays all security issues, organized in folders (colored tabs) in an issues pane. Issues are organized based on settings in Micro Focus Fortify Software Security Center. To the right of the issues pane are four tabs that provide information specific to the issue selected in the issues pane.



Folders contain logically defined sets of issues. For example, the **Critical** folder contains all critical issues for a project. Similarly, the **Low** folder contains all low-priority issues.

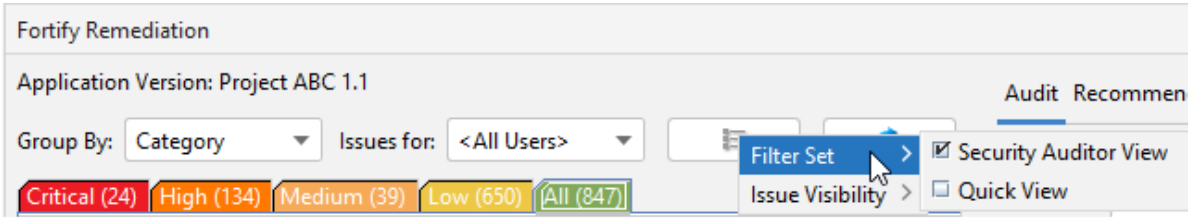
Filters determine which issues are visible. Filters are organized into distinct groups called filter sets. An issue template can contain definitions for multiple filter sets. You can use multiple filter sets to change the sorting and visibility of issues.

To remediate issues, the project you have open in the IDE must correspond to the application version you opened from Fortify Software Security Center (see "Opening Fortify Software Security Center Application Versions" on page 37).

Viewing and Selecting Issues

To view and select issues in an opened application version:

1. Click **Change View Options**( ).



2. From **Filter Set**, select one of the following filter sets to apply to issues:
   - Select **Security Auditor View** to list all issues relevant to a security auditor.
   - Select **Quick View** to list only issues in the **Critical** folder (these have a potentially high impact and a high likelihood of occurring) and the **High** folder (these have a potentially high impact and a low likelihood of occurring).

   Note: The filter sets available depends on the issue template assigned to the application version you opened.

3. From the **Group By** list, select a value to use to sort issues in all visible folders into groups.

   The default grouping is **Category**. For a description of the available **Group By** options, see "Grouping Issues" on page 41.

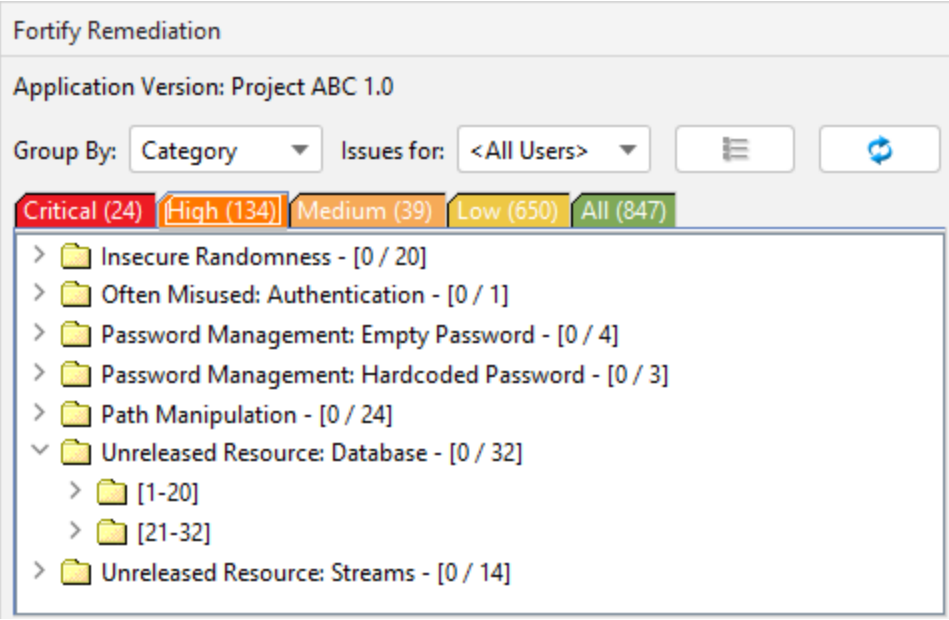
4. By default, issues assigned to your Micro Focus Fortify Software Security Center user name are shown. From the **Issues for** list, you can select one of the following:
   - **<All Users>**
   - A Fortify Software Security Center user name
5. Click a color-coded tab (folder) to view the associated issues.

   Note: The tabs shown depends on your **Filter Set**, **Group By**, and **Issues for** selections. It is possible that not all tabs are shown. The tabs shown also depends on the issue template associated with the application version.

   - The **Critical** tab contains issues that have a high impact and a high likelihood of exploitation. Fortify recommends that you remediate critical issues immediately.
   - The **High** tab contains issues that have a high impact and a low likelihood of exploitation. Fortify recommends that you remediate high issues with the next patch release.
   - The **Medium** tab contains issues that a have low impact and a high likelihood of exploitation. Fortify recommends that you remediate medium issues as time permits.
   - The **Low** tab contains issues that have a low impact and a low likelihood of exploitation. Fortify recommends that you remediate low issues as time permits (your organization can customize this category).
   - The **All** tab contains all issues.

   Within each color-coded tab, issues are grouped into folders. After each folder name, enclosed in brackets, is the number of audited issues and the total number of issues in the folder. For example, **Command Injection - [1 / 3]** indicates that one issue out of three categorized as Command Injection has been audited.
6. Click to expand a folder and view the associated issues.

   The Remediation Plugin retrieves the corresponding issues from Fortify Software Security Center.



Note: By default, if a folder contains more than 20 issues, the issues are grouped into subfolders in blocks of 20 with folder names that indicate the issues included. For example, if a folder contains 32 issues, the first 20 issues are in a subfolder labeled **[1-20]** and the last set of issues are in a subfolder labeled **[21-32]**. To change the default pagination setting of 20, set the `com.fortify.remediation.PaginationCount` property. You can also disable issue pagination by setting the `com.fortify.remediation.PaginateIssues` property to `false`. For more information about these properties, see the *Micro Focus Fortify Static Code Analyzer Tools Properties Reference Guide*.

7. Select an issue to view the issue information.

Grouping Issues

The items visible in the Fortify Remediation window issues pane vary depending on the selected grouping option. The value you select from the **Group By** list sorts issues in all visible folders into subfolders. Use the **Group By** options to group and view the issues in different ways. The following table describes the available **Group By** options.

Option	Description
Analysis	Groups issues by the audit analysis, such as Suspicious, Exploitable, and Not an Issue.
Analysis Type	Groups issues by analyzer product, such as SCA, WEBINSPECT, and SECURITYSCOPE (WebInspect Agent).

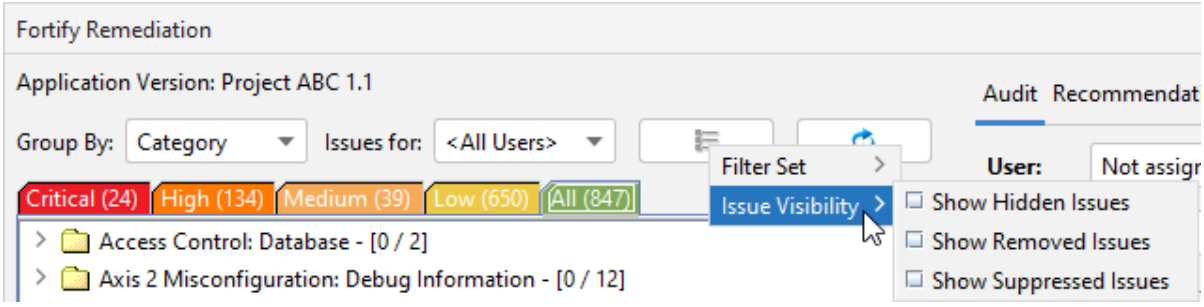
Option	Description
Analyzer	Groups issues by analyzer group, such as Control Flow, Data Flow, Pentest, and Structural.
App Defender Protected	Groups issues by whether Application Defender can protect the vulnerability category.
Category	Groups issues by vulnerability category. This is the default setting.
<custom_tagname>	Groups issues by custom tag.
File Name	Groups issues by file name.
Folder	Groups issues by folders defined in the issue template.
Fortify Priority Order	Groups issues as Critical, High, Medium, and Low based on the analyzer's combined values of impact and likelihood.
Introduced date	Groups issues by the date the issue was first detected.
Issue State	Groups audited issues by whether the issue is an open issue or not an issue based on the level of analysis set for the primary tag. Values equivalent to suspicious and exploitable are considered open issue states.
Kingdom	Groups issues by the Seven Pernicious Kingdoms classification.
Manual	Groups issues by whether they were manually created by penetration test tools, and not automatically produced by a web crawler such as Fortify WebInspect.
<metadata_listname>	Groups issues using the alternative metadata external list names (for example, OWASP Top 10 *<year>*, CWE, PCI SSF *<version>*, STIG *<version>*, and others).
New Issue	Shows which issues are new since the last scan. For example, if you run a new scan, any issues that are new display in the tree under the **NEW** group and the others are displayed in the **UPDATED** group. If removed issues are visible, issues not found in the latest scan are displayed in the **REMOVED** list.
Package	Groups issues by package or namespace. Does not appear for projects for which this option is not applicable, such as C projects.

Option	Description
Primary Context	Groups issues where the primary location or sink node function call occurs in the same code context.
Sink	Groups issues that share the same dataflow sink function.
Source	Groups issues that share the same dataflow source functions.
Source Context	Groups dataflow issues that have the source function call contained in the same code context.
Source File	Groups dataflow issues by the source code file where the taint originated.
Status	Groups issues by the audit status (**Reviewed**, **Unreviewed**, or **Under Review**).
Taint Flag	Groups issues by the taint flags that they contain.
URL	Groups dynamic issues by the request URL.

Customizing Issue Visibility

You can customize the issues pane to determine which issues the Remediation Plugin displays.

1. Click **Change View Options** ( ).



2. From **Issue Visibility**, choose from the following options:
   - To display all hidden issues, select **Show Hidden Issues**.

     Note: The visibility filter settings in the issue template associated with the application version determine which issues are hidden.

   - To display all the issues removed since the previous analysis, select **Show Removed Issues**.

- To display all suppressed issues, select **Show Suppressed Issues**.

  Note: Users who audit issues can suppress specific types of issues that are not considered high priority or of immediate concern. For example, auditors can suppress issues that are fixed, or issues that your organization plans not to fix.

The Fortify Remediation Plugin displays issues based on your selection.

Note: You can also specify the issue visibility settings from the Options dialog box (select **Fortify > Remediation Options**).

Searching for Issues

You can use the search box below the issues list to search for issues. After you type a search query, either press **Enter** or click the magnifying glass icon to start the search and filter the issues in the tree. After you type a search term, the label next to the folder name changes to indicate the number of issues that match the search as a subset of the total. For example, Hot (2 of 5).

To indicate the type of comparison to perform, wrap search terms with delimiters. The following table describes the syntax to use for the search string.

Comparison	Description
contains	Searches for a term without any special qualifying delimiters
equals	Searches for an exact match when you enclose the term in quotation marks (`""`)
number range	Searches for a range of numbers using the standard mathematical interval notation of parentheses and/or brackets to indicate whether the endpoints are excluded or included respectively Example: `(2,4]` indicates greater than two and less than or equal to four
not equal	Excludes issues specified by the string when you precede the string with the exclamation character (`!`) Example: `file:!Main.java` returns all issues that are not in `Main.java`

You can further qualify search terms with modifiers. The syntax to use for a modifier is `modifier:<search_term>`.

If you specify more than one modifier, the search returns only issues that match all the modified search terms. For example, `file:ApplicationContext.java category:SQL Injection` returns only SQL injection issues found in `ApplicationContext.java`.

If you use the same modifier more than once in a search string, then the search terms qualified by those modifiers are treated as an `OR` comparison. For example, `file:ApplicationContext.java`

`category:SQL Injection category:Cross-Site Scripting` returns SQL injection issues and cross-site scripting issues found in `ApplicationContext.java`.

For complex searches, you can also insert the AND or the OR keyword between your search queries. Note that AND and OR operations have the same priority in searches.

Search Modifiers

You can use a search modifier to specify to which attribute of an issue the search term applies. To use a modifier that contains a space in the name, such as the name of the custom tag, you must enclose the modifier in brackets. For example, to search for issues that are new, type `[issue age]:new`.

A search that is not qualified by a modifier tries to match the search string on the following issue attributes: kingdom, primary rule id, analyzer, filename, severity, class name, function name, instance id, package, confidence, type, subtype, taint flags, category, sink, and source. For example:

- To apply the search to all modifiers, type a string such as `control flow`. This searches all the modifiers and returns any result that contains the specified string.
- To apply the search to a specific modifier, type the modifier name and the string as follows: `analyzer:control flow`. This returns all results whose analyzer is `control flow`.

The following table describes the search modifiers. A few modifiers have a shortened modifier name indicated in parentheses in the Modifier column. You can use either modifier string.

Modifier	Description
`accuracy`	Searches for issues based on the accuracy value specified (0.1 through 5.0).
`analysis`	Searches for issues that have the specified audit analysis value, such as `exploitable`, `not an issue`, and so on.
`[analysis type]`	Searches for issues by analyzer product such as `SCA` and `WEBINSPECT`.
`analyzer`	Searches the issues for the specified analyzer such as `control flow`, `data flow`, `structural`, and so on.
`[app defender protected]` (`def`)	Searches for issues based on whether Application Defender can protect the vulnerability category (`protected` or `not protected`).
`[attack payload]`	Searches for issues that contain the search term in the part of the request that caused the vulnerability for penetration test results.

Modifier	Description
`[attack type]`	Searches for issues based on the type of penetration test attack conducted (`URL`, `parameter`, `header`, or `cookie`).
`audience`	Searches for issues by intended audience, such as `dev`, `targeted`, `medium`, `broad`, and so on. **Note:** This metadata is legacy information that is no longer used and will be removed in a future release. Fortify recommends that you do not use this search modifier.
`audited`	Searches the issues to find `true` if the primary tag is set and `false` if the primary tag is not set. The default primary tag is the Analysis tag.
`body`	Searches for issues that contain the search term in the HTTP message body in penetration test results, which is all the data that is transmitted immediately following the headers.
`category (cat)`	Searches for the specified category or category substring.
`class`	Searches for issues based on the specified class name.
`comments (comment, com)`	Searches for issues that contain the search term in the comments that have been submitted on the issue.
`commentuser`	Searches for issues with comments from a specified user.
`confidence (con)`	Searches for issues that have the specified confidence value. The confidence value is based on the number of assumptions made in the code analysis. The more assumptions made, the lower the confidence value.
`cookies`	Searches for issues that contain the search term in the cookie from the HTTP query for penetration test results.
`correlated`	Searches for issues based on whether the issues are correlated with another analyzer.
`[correlation group]`	Searches for issues based on whether the issues are in the same correlation group.
<custom_tagname>	Searches for issues based on the value of the specified custom

Modifier	Description
	tag. You can search a list-type custom tag using a range of values. The values of a list-type custom tag are an enumerated list where the first value is 0, the second is 1, and so on. You can use the search syntax for a range of numbers to search for ranges of list-type custom tag values. For example, `analysis:[0,2]` returns the issues that have the values of the first three Analysis values, 0, 1, and 2 (Not an Issue, Reliability Issue, and Bad Practice). To search a date-type custom tag, specify the date in the format: yyyy-mm-dd.
`file`	Searches for issues where the primary location or sink node function call occurs in the specified file.
`[fortify priority order]`	Searches for issues that have a priority level that matches the specified priority determined by the analyzer. Valid values are `critical`, `high`, `medium`, and `low`, based on the expected *impact* and *likelihood* of exploitation. The impact value indicates the potential damage that might result if an issue is successfully exploited. The likelihood value is a combination of confidence, accuracy of the rule, and probability that an attacker can exploit the issue.
`headers`	Searches for issues that contain the search term in the request header for penetration test results.
`historyuser`	Searches for issues that have audit data modified by the specified user.
`[http version]`	Searches for issues based on the specified HTTP version such as `HTTP/1.1`.
`impact`	Searches for issues based on the impact value specified (0.1 through 5.0).
`[instance id]`	Searches for an issue based on the specified instance ID.
`[issue age]`	Searches for the issue age, which is either `new`, `updated`, `reintroduced`, or `removed`.

Modifier	Description
`[issue state]`	Searches for audited issues based on whether the issue is an open issue or not an issue (determined by the level of analysis set for the primary tag).
`kingdom`	Searches for all issues in the specified kingdom.
`likelihood`	Searches for issues based on the specified likelihood value (0.1 through 5.0).
`line`	Searches for issues on the primary location line number. For dataflow issues, the value is the sink line number. Also see "sourceline" on page 50.
`manual`	Searches for issues based on whether they were manually created by penetration test tools, and not automatically produced by a web crawler such as WebInspect.
`[mapped category]`	Searches for issues based on the specified category that is mapped across the various analyzers (Fortify Static Code Analyzer, Fortify WebInspect, and Fortify WebInspect Agent).
`maxconf`	Searches for all issues that have a confidence value equal to or less than the number specified as the search term.
`maxVirtConf`	Searches for dataflow issues that have a virtual call confidence value equal to or less than the number specified as the search term.
<metadata_listname>	Searches for issues based on the value of the specified metadata external list (for example, `[owasp top 10 <year>]`, `[cwe top 25 <year>]`, `[pci ssf <version>]`, `[stig <version>]`, and others).
`minconf`	Searches for all issues that have a confidence value equal to or greater than the number specified as the search term.
`method`	Searches for issues based on the method, such as `GET`, `POST`, and so on.
`min_virtual_call_confidence (virtconf, minVirtConf)`	Searches for dataflow issues that have a virtual call confidence value equal to or greater than the number specified as the search term.

Modifier	Description
`package`	Searches for issues where the primary location occurs in the specified package or namespace. For dataflow issues, the primary location is the sink function.
`parameters`	Searches for issues that contain the search term in the HTTP query parameters.
`primary`	Searches for issues that have the specified primary tag value. By default, the primary tag is the Analysis tag.
`[primary context]`	Searches for issues where the primary location or sink node function call occurs in the specified code context. Also see "sink" below and "[source context]" below.
`primaryrule (rule)`	Searches for all issues related to the specified sink rule.
`probability`	Searches for issues based on the probability value specified (1.0 through 5.0).
`remediation effort`	Searches for issues based on the remediation effort value specified. The valid values are whole numbers from 1.0 to 12.0.
`response`	Searches for issues that contain the search term in the response from the protocol used in penetration test results.
`severity (sev)`	Searches for issues based on the specified severity value (legacy metadata).
`sink`	Searches for issues that have the specified sink function name. Also see "[primary context]" above.
`source`	Searches for dataflow issues that have the specified source function name. Also see "[source context]" below.
`[source context]`	Searches for dataflow issues that have the source function call contained in the specified code context. Also see "source" above and "[primary context]" above.
`sourcefile`	Searches for dataflow issues with the source function call that the specified file contains. Also see "file" on page 47.

Modifier	Description
`sourceline`	Searches for dataflow issues having taint source entering the flow on the specified line.
`status`	Searches issues that have the status `reviewed`, `not reviewed`, or `under review`.
`suppressed`	Searches for suppressed issues.
`taint`	Searches for issues that have the specified taint flag.
`trigger`	Searches for issues that contain the search term in the part of the response that shows that a vulnerability occurred for penetration test results.
`url`	Searches for issues based on the specified URL.
`user`	Searches for issues assigned to the specified user.

Search Query Examples

Consider the following search query examples:

- To search for all privacy violations in file names that contain `jsp` with `getSSN()` as a source, type the following:

  ```
  category:"privacy violation" source:getssn file:jsp
  ```
- To search for all file names that contain `com/fortify/awb`, type the following:

  ```
  file:com/fortify/awb
  ```
- To search for all paths that contain traces with `mydbcode.sqlcleanse` as part of the name, type the following:

  ```
  trace:mydbcode.sqlcleanse
  ```
- To search for all paths that contain traces with `cleanse` as part of the name, type the following:

  ```
  trace:cleanse
  ```
- To search for all issues that contain `cleanse` as part of any modifier, type the following:

  ```
  cleanse
  ```
- To search for all suppressed vulnerabilities with `asdf` in the comments, type the following:

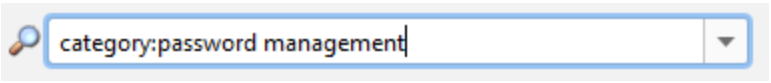
  ```
  suppressed:true comments:asdf
  ```
- To search for all categories except for SQL Injection, type the following:

  ```
  category:!SQL Injection
  ```

Performing Searches

To use the search box to perform a simple search, do one of the following:

- Type a search string in the box and press **Enter**.



- To select a search query you used before, click the arrow in the search box, and then select a search term from the list.

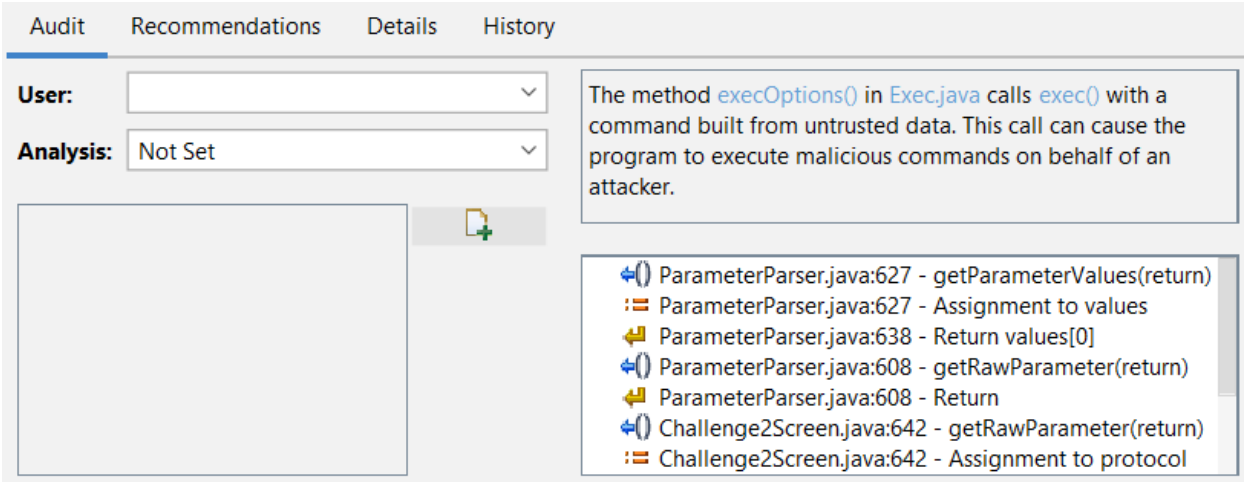
Viewing Issue Information

After you select an issue, the Fortify Remediation Plugin displays the issue-specific content on the **Audit**, **Recommendations**, **Details**, and **History** tabs.

Audit Tab

The **Audit** tab provides a dashboard of analysis information for the selected issue.

Note: Any changes you make on the **Audit** tab are automatically uploaded to the application version on Micro Focus Fortify Software Security Center.



The following table describes the **Audit** tab features.

Element	Description
User	The user assigned to the selected issue. If the box is empty, no user is assigned to the selected issue. To assign a user to the issue, see "Assigning Users to Issues" on page 56.

Element	Description
Analysis	Your assessment for the selected issue. To change the assessment, select an item from the list. This is the primary tag defined in Fortify Software Security Center for the application. The default name of this tag is **Analysis**, but it might be different for your organization.
<custom_ tagname>	Any custom tags your organization has defined in Fortify Software Security Center. If available, these are displayed below the **Analysis** (primary) tag. If the audit results have been submitted to Audit Assistant in Fortify Software Security Center, then in addition to any other custom tags, the tab displays the following tags: • **AA_Prediction**—Exploitability level that Audit Assistant assigned to the issue. You cannot modify this tag value. • **AA_Confidence**—Confidence level from Audit Assistant for the accuracy of its AA_Prediction value. This is a percentage, expressed in values that range from 0.000 to 1.000. For example, a value of 0.982 indicates a confidence level of 98.2 percent. You cannot change this tag value. • **AA_Training**—Whether to include or exclude the issue from Audit Assistant training. You can modify this value. For more information about Audit Assistant, see the *Micro Focus Fortify Software Security Center User Guide*.
Issue Abstract (top right)	A summary of the selected issue.
Analysis Trace (bottom right)	The items of evidence that the analyzer uncovered. The analysis trace is presented in the order it was discovered. For descriptions of the analysis trace icons, see "Analysis Trace" below
Comments (bottom left)	Any additional information added to the issue. For instructions on how to add comments, see "Adding Comments to Issues" on page 56.

See Also

"Updating Audit Information" on page 55

Analysis Trace

This trace on the **Audit** tab is presented in sequential order. For dataflow issues, this trace is a presentation of the path that the tainted data follows from the source function to the sink function.

For example, when you select an issue that is related to potentially tainted dataflow, the analysis trace box shows the direction of the dataflow in this section of the source code.

The analysis trace box uses the icons described in the following table to show how the dataflow moves in this section of the source code or execution order.

Icon	Description
	Data is assigned to a field or variable
	Information is read from a source external to the code (HTML form, URL, and so on)
	Data is assigned to a globally scoped field or variable
	A comparison is made
	The function call receives tainted data
	The function call returns tainted data
	Passthrough, tainted data passes from one parameter to another **Note:** This is typically shown as functionA(x : y) to indicate that data is transferred from x to y. The x and y values are either: • An argument index • `return`—The return value of a function • `this`—The instance of the current object • A specific object field or key
	An alias is created for a memory location
	Data is read from a variable
	Data is read from a global variable
	Tainted data is returned from a function
	A pointer is created

Icon	Description
	A pointer is dereferenced
	The scope of a variable ends
	The execution jumps
	A branch is taken in the code execution
	A branch is not taken in the code execution
	Generic
	A runtime source, sink, or validation step
	Taint change

The Analysis Trace box can contain inductions. Inductions provide supporting evidence for their parent nodes. Inductions consist of:

- A text node displayed in italics as a child of the trace node. This text node is expanded by default.
- An induction trace, displayed as a child of the text node.

To display the induction reference information for that induction, click it.

Recommendations Tab

The **Recommendations** tab provides suggestions and examples on how to secure a vulnerability or remedy a bad practice. The following table describes the sections on this tab.

Section	Description
Recommendations/Custom Recommendations	Describes possible solutions for the selected issue. It can also include examples and recommendations that your organization has defined.
Tips/Custom Tips	Provides useful information specific to the selected issue, and any custom tips that your organization has defined.
References/Custom References	Lists references for the recommendations provided, including any custom references that your organization has defined.

Details Tab

The **Details** tab provides an abstract of the selected issue description, a detailed explanation, and examples. The following table describes the sections on this tab.

Section	Description
Abstract/Custom Abstract	Displays a summary of the selected issue, including custom abstracts defined by your organization.
Explanation/Custom Explanation	Displays a description of the conditions under which an issue of the selected type occurs. This includes a discussion of the vulnerability, the constructs typically associated with it, ways in which attackers can exploit it, and the potential ramifications of an attack. This section also provides custom explanations defined by your organization.
Instance ID	A unique identifier for the issue.
Primary Rule ID	The identifier for the primary rule used to uncover the issue.
Priority Metadata Values	Priority metadata values for the issue.
Legacy Priority Metadata Values	Legacy priority metadata values for the issue.
Remediation Effort	The relative amount of effort required to fix and verify the issue.

History Tab

The **History** tab displays a history of audit actions, including details such as the time and date, and the name of the user who modified the issue.

Updating Audit Information

After you select an issue, you can update the audit information on the **Audit** tab. To see any updates to the audit results made on Micro Focus Fortify Software Security Center, click **Refresh** ( ).

Assigning Users to Issues

To assign a user to an issue:

1. From a folder in the issues pane, select an issue.
2. Select the **Audit** tab, and then, from the **User** list, select a user name.

   To leave the issue unassigned, select the blank value from the list.

The Fortify Remediation Plugin makes the update to the application version on Micro Focus Fortify Software Security Center.

Assigning Tags to Issues

To assign tag values to an issue:

1. From a folder in the issues pane, select an issue.
2. From the **Analysis** list on the **Audit** tab, select a value that reflects your evaluation of this issue.

   This is the primary tag as defined in Micro Focus Fortify Software Security Center. The default name of this tag is **Analysis**, but it might be different for your organization.
3. If custom tags defined for the project exist, provide values for them.

   The Remediation Plugin displays all custom tags assigned to the application; however, you can only provide values for tags that your Fortify Software Security Center user account has permission to edit.

   Text-type custom tags accept up to 500 characters (HTML/XML tags and newlines are not allowed).

   For date-type custom tags, type a date or click ( ) to select a date from a calendar.

The Fortify Remediation Plugin makes the updates to the application version on Fortify Software Security Center.

Adding Comments to Issues

The comments box below the **Analysis** (primary tag) list displays any comments submitted for the selected issue.

To add a comment to an issue:

1. From a folder in the issues pane, select an issue.
2. From the **Audit** tab, click **Add Comment** ( ).
3. In the Add Comment for Issue dialog box, type your comment.
4. Click **OK**.

The Fortify Remediation Plugin makes the updates to the application version on Micro Focus Fortify Software Security Center.

Locating Issues in your Source Code

Because the Fortify Remediation Plugin works as a plugin to IntelliJ IDEA, Android Studio, PyCharm, and WebStorm, you can use it to locate security-related issues in your code. You must have the same project open in the IDE as you selected from Micro Focus Fortify Software Security Center with the Fortify Remediation Plugin.

To locate issues in the source code, do one of the following:

- Select an issue from the issues pane.
- From the **Audit** tab, select an issue from the Analysis Trace box.

The IDE places the focus on the line of code that contains the security-related issue displayed in the Fortify Remediation Plugin.

Locating Remediation Plugin Log Files

For help diagnosing a problem with the Remediation Plugin, provide the log file to Micro Focus Fortify Customer Support. The default location of the log file is:

- On Windows:

  `C:\Users\<username>\AppData\Local\Fortify\IntelliJRemediation-<version>\log`
- On Linux and macOS:

  `<userhome>/.fortify/IntelliJRemediation-<version>/log`

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 User Guide (Fortify Plugins for JetBrains IDEs and Android Studio 22.1.0)

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!