
Micro Focus

Fortify Plugins for JetBrains IDEs

Software Version: 20.1.0

User Guide

Document Release Date: May 2020

Software Release Date: May 2020



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

© Copyright 2012 - 2020 Micro Focus or one of its affiliates

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 April 16, 2020. 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-and-services/documentation>

Contents

Preface	5
Contacting Micro Focus Fortify Customer Support	5
For More Information	5
About the Documentation Set	5
Change Log	6
Chapter 1: Introduction	7
Fortify Plugins for JetBrains IDEs	7
Related Documents	7
All Products	8
Micro Focus Fortify Software Security Center	8
Micro Focus Fortify Static Code Analyzer	9
Chapter 2: Using the Fortify Analysis Plugin	10
About the Fortify Analysis Plugin Installation	10
Installing the Fortify Analysis Plugin	10
Uninstalling the Fortify Analysis Plugin	11
Fortify Security Content	11
Updating Fortify Security Content	12
Updating Fortify Security Content on a Network That Uses a Proxy Server	12
Analysis Configuration	13
Setting Memory for Code Analysis	13
Setting the Query Language Type	13
Selecting the Fortify Security Content to Apply During Analysis	14
Using Quick Scan Mode for Project Analysis	14
Enabling FindBugs During Scans	15
Excluding Dependent Modules from Analysis	15
Specifying Additional Fortify Static Code Analyzer Options	15
Synchronizing with Fortify Software Security Center	16
Scanning Projects	16
Scanning Large and Complex Projects	17

Performing an Advanced Scan	17
Uploading Analysis Results to Fortify Software Security Center	18
Troubleshooting the Analysis Plugin	19
Chapter 3: Using the Fortify Remediation Plugin	20
About the Fortify Remediation Plugin Installation	20
Installing the Fortify Remediation Plugin	20
Uninstalling the Fortify Remediation Plugin	21
Opening Fortify Software Security Center Application Versions	21
Viewing Audit Results	22
Grouping and Selecting Issues	22
Grouping Issues	23
Viewing Issue Information	25
Audit Tab	25
Recommendations Tab	26
Details Tab	26
History Tab	27
Assigning Users to Issues	27
Assigning Tags to Issues	27
Adding Comments to Issues	28
Customizing Issue Visibility	28
Searching for Issues	29
Search Modifiers	29
Locating Issues in Your Source Code	35
Troubleshooting the Remediation Plugin	35
Send Documentation Feedback	36

Preface

Contacting Micro Focus Fortify Customer Support

You can contact Micro Focus Fortify Customer Support, manage your Support cases, acquire licenses, and manage your account on the following website:

<https://softwaresupport.softwaregrp.com>

For More Information

For more information about Fortify software products:

<https://software.microfocus.com/solutions/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-and-services/documentation>

Change Log

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

Document Release / Document Version	Change
20.1.0	Updated: <ul style="list-style-type: none">• "Troubleshooting the Analysis Plugin" on page 19 and "Troubleshooting the Remediation Plugin" on page 35 - Added the location of log files
19.2.0	Updated: <ul style="list-style-type: none">• "Viewing Issue Information" on page 25 - Updates made to reflect the changed tab names• Updates made to reflect support with PyCharm IDE
19.1.0	Updated: Release date and version
18.20	Updated: Release date and version

Chapter 1: Introduction

This section contains the following topics:

Fortify Plugins for JetBrains IDEs	7
Related Documents	7

Fortify Plugins for JetBrains IDEs

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 Micro Focus Fortify Static Code Analyzer
- Review the analysis results to eliminate false positives and prioritize the order of remediation
- Fix and eliminate security vulnerabilities in your code (remediation)
- Integrate with Micro Focus Fortify Software Security Center

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	Fortify Analysis Plugin
Upload scan results to Fortify Software Security Center	Fortify Analysis Plugin
Integrate with Fortify Software Security Center	Fortify Remediation Plugin
Review security issues, add comments, and assign users	Fortify Remediation Plugin

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-and-services/documentation>. All guides are available in both PDF and HTML formats.

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
<i>About Micro Focus Fortify Product Software Documentation</i>	This paper provides information about how to access Micro Focus Fortify product documentation.
<i>About_Fortify_Docs_<version>.pdf</i>	Note: This document is included only with the product download.
<i>Micro Focus Fortify Software System Requirements</i>	This document provides the details about the environments and products supported for this version of Fortify Software.
<i>Fortify_Sys_Reqs_<version>.pdf</i>	
<i>Micro Focus Fortify Software Release Notes</i>	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.
<i>FortifySW_RN_<version>.pdf</i>	
<i>What's New in Micro Focus Fortify Software <version></i>	This document describes the new features in Fortify Software products.
<i>Fortify_Whats_New_<version>.pdf</i>	

Micro Focus Fortify Software Security Center

The following documents provide 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
<i>Micro Focus Fortify Software Security Center User Guide</i>	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.
<i>SSC_Guide_<version>.pdf</i>	It is intended for use by system and instance

Document / File Name	Description
	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
<i>Micro Focus Fortify Static Code Analyzer User Guide</i> 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.
<i>Micro Focus Fortify Static Code Analyzer Custom Rules Guide</i> 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 the analysis phase that enables developers to quickly and easily identify vulnerabilities in their 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 scanning options and connect to Micro Focus Fortify Software Security Center. Your organization can use the plugin scan results with 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 how to upload the analysis results to Fortify Software Security Center.

This section contains the following topics:

About the Fortify Analysis Plugin Installation	10
Fortify Security Content	11
Analysis Configuration	13
Scanning Projects	16
Uploading Analysis Results to Fortify Software Security Center	18
Troubleshooting the Analysis Plugin	19

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. In the left panel, 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. In the left panel, 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*.

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 either `fortifyupdate.cmd` (on a Windows system) or `fortifyupdate` (on a non-Windows system). 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 either `fortifyupdate.cmd -import <zip_file>` (on a Windows system) or `fortifyupdate -import <zip_file>` (on a non-Windows system).

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 Host**, 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 either `fortifyupdate.cmd` (on a Windows system) or `fortifyupdate` (on a non-Windows system).

Analysis Configuration

You can modify Fortify Analysis Plugin settings to do the following:

- Specify the amount of memory to use during scans
- Specify the procedural language your SQL files use
- Determine the security content to use in project analysis

This controls what Micro Focus Fortify Static Code Analyzer looks for during a scan.

- Configure advanced analysis options (for example, enable quick scan mode)
- Configure a connection to Micro Focus Fortify Software Security Center

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. Open your IntelliJ IDEA or Android Studio project.
2. From the menu bar, select **Fortify > Analysis Settings**.

The Fortify Analysis Settings dialog box opens to the **Analysis Configuration** tab.

3. 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 prevents you from specifying more memory than is physically available on your system.

4. 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. (Fortify Static Code Analyzer determines the SQL type setting by the `com.fortify.sca.fileextension.sql` property in the `fortify-sca.properties` file.)

To set the procedural language for analysis:

1. Open your IntelliJ IDEA or Android Studio project.
2. From the menu bar, select **Fortify > Analysis Settings**.

The Fortify Analysis Settings dialog box opens to the **Analysis Configuration** tab.

3. Under **Scan Configuration**, from the **SQL type** list, select **TSQL** or **PLSQL**.
4. 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. Open your IntelliJ IDEA or Android Studio project.
2. From the menu bar, select **Fortify > Analysis Settings**.
The Fortify Analysis Settings dialog box opens to the **Analysis Configuration** tab.
3. Under **Security Content**, clear the **Use all installed security content** check box.
4. In the **Installed Fortify Security Content** list, select the check boxes for the rules to apply during the scan.
5. 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.
6. Click **OK**.

Using Quick Scan Mode for Project Analysis

Quick scan mode provides a way to quickly scan your projects for major issues. In quick scan mode, Analysis Plugin searches for high-confidence, high-severity issues. Quick scans are a great way to get many applications through an assessment so that you can quickly find issues and begin remediation. Although the scan is faster than a full scan, it does not provide as robust a result set. For example, a quick scan of the WebGoat sample application uncovers approximately 75% fewer issues than a full scan of the same application. Critical and other issues that a quick scan cannot detect might exist in your application. Fortify recommends that you run full scans whenever possible. For more details about the configuration of quick scan mode, see the *Micro Focus Fortify Static Code Analyzer User Guide*.

Note: By default, Micro Focus Fortify Software Security Center ignores uploaded 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. Open your IntelliJ IDEA or Android Studio project.
2. From the menu bar, select **Fortify > Analysis Settings**.
3. Click the **Advanced Options** tab.
4. Select the **Enable quick scan mode** check box.
5. Click **OK**.

Enabling FindBugs During Scans

FindBugs is a static analysis tool that detects quality issues in Java code. You can run FindBugs with the Analysis Plugin. The results are integrated into the analysis results file.

Unlike Micro Focus Fortify Static Code Analyzer, which analyzes Java source files, FindBugs analyzes Java bytecode. Therefore, you must successfully compile your project before you run a scan with FindBugs enabled. Otherwise, FindBugs is not run with the scan and Fortify Static Code Analyzer issues a warning to that effect.

To enable FindBugs for your scan:

1. Open your IntelliJ IDEA or Android Studio project.
2. From the menu bar, select **Fortify > Analysis Settings**.
3. Click the **Advanced Options** tab.
4. Select the **Enable FindBugs integration** check box.
5. 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, scan results are more accurate if you scan an entire project at once.

To exclude dependent or nested modules from analysis:

1. Open your IntelliJ IDEA or Android Studio project.
2. From the menu bar, select **Fortify > Analysis Settings**.
3. Click the **Advanced Options** tab.
4. Clear the **Scan resources in dependent modules** check box.
5. Click **OK**.

Specifying Additional Fortify Static Code Analyzer Options

To specify additional Micro Focus Fortify Static Code Analyzer options:

1. Open your IntelliJ IDEA or Android Studio project.
2. From the menu bar, select **Fortify > Analysis Settings**.
3. Click the **Advanced Options** tab.
4. Select the **Use Additional SCA Arguments** check box.
5. 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 on the available command-line options and syntax, see the *Micro Focus Fortify Static Code Analyzer User Guide*.

6. To change the output location for your scan results, click the button next to the **Output results to** box, and then, in the Select output directory dialog box, specify the directory in which to save the analysis results.
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 re-scan 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. Open your IntelliJ IDEA or Android Studio project.
2. From the menu bar, select **Fortify > Analysis Settings**.
3. Click the **Synchronize Options** tab.
4. In the **Server URL** box, specify the URL for your Fortify Software Security Center server (for example, `http://127.0.0.1:8180/ssc`).
5. If required, specify a proxy server and port number.
6. Select the **Synchronize project with server** check box.
7. Click **OK**.

Scanning Projects

This section provides information about how to use the Fortify Analysis Plugin to scan and analyze your Java source code 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 12.

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 scan 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:

1. Open your IntelliJ IDEA or Android Studio project.
2. Do one of the following:
 - From the menu bar, select **Fortify > Analyze Project**.
 - Right-click a module, and then select **Analyze Module** from the context menu.

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**.

The Micro Focus 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 FPR.

If you configured a connection to Micro Focus Fortify Software Security Center, the Fortify Analysis Plugin displays the Select Software Security Center Application Version dialog box. If you have not already set up a connection to Fortify Software Security Center, you can do so later, and then upload the scan results (see "[Uploading Analysis Results to Fortify Software Security Center](#)" on the next page).

3. If you want to upload your scan results to Fortify Software Security Center, select the Fortify Software Security Center application version that corresponds to your project, and then click **OK**.

Scanning Large and Complex Projects

Exceptionally large code bases might require that you take measures to ensure a complete scan, including using Micro Focus Fortify Static Code Analyzer to scan the code in smaller sections. By default, your project modules are translated separately, and the results are combined into a single FPR file during the analysis phase.

While you can edit Fortify Static Code Analyzer command options, you can handle large and complex scans more successfully directly through the command console. You can use the Advanced Scan wizard 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.

Performing an Advanced Scan

To perform an advanced scan:

1. Open your IntelliJ IDEA or Android Studio project.
2. From the menu bar, select **Fortify > Advanced Scan**.

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

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.

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

4. The Fortify Analysis Plugin automatically detects the class path from IntelliJ or Android Studio settings for the project. 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** from the shortcut menu.
5. From the **Java version** list, select the Java version for the project.
6. In the **Build ID** box, type the build ID.
The project name is the default build ID with unacceptable file system symbols escaped.
7. 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.
8. To perform a quick scan, select the **Enable Quick Scan mode** check box.
For information about quick scans, see "[Using Quick Scan Mode for Project Analysis](#)" on page 14.
9. Click **Next**.
The scan process includes the following phases:
 - During the *clean* phase, Fortify Static Code Analyzer removes files from 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 scans source files identified during the translation phase and generates analysis results in the FPR format.
10. (Optional) To skip a scanning 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.
11. 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 scan is completed. However, before you do, a corresponding application version must already exist in Fortify Software Security Center.

Note: By default, Micro Focus Fortify Software Security Center ignores uploaded 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. Check to make sure that you have a generated FPR file in the default location or the location configured in the Fortify Analysis Settings dialog box (see step 6 in ["Specifying Additional Fortify Static Code Analyzer Options" on page 15](#)).
The FPR file must already exist.
2. From the IntelliJ IDEA or Android Studio menu bar, select **Fortify > Upload Results to Software Security Center**.
The Software Security Center Credentials dialog box opens.
3. Provide the Fortify Software Security Center server URL and your Fortify Software Security Center credentials, and then click **OK**.
4. Select the Fortify Software Security Center application version that corresponds to your IntelliJ IDEA project, and then click **OK**.

You can now open the application and view the results from Fortify Software Security Center or from the Fortify Remediation Plugin. For information about how to view and work with scan 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 scan results from IntelliJ or Android Studio, see ["Using the Fortify Remediation Plugin" on page 20](#).

Troubleshooting the Analysis Plugin

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
 - C:\Users\<username>\AppData\Local\Fortify\IntelliJAnalysis-<version>\log
- On Linux and macOS:
 - <userhome>/.fortify/sca<version>/log
 - <userhome>/.fortify/IntelliJAnalysis-<version>/log

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	20
Opening Fortify Software Security Center Application Versions	21
Viewing Audit Results	22
Viewing Issue Information	25
Assigning Users to Issues	27
Assigning Tags to Issues	27
Adding Comments to Issues	28
Customizing Issue Visibility	28
Searching for Issues	29
Locating Issues in Your Source Code	35
Troubleshooting the Remediation Plugin	35

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 panel, 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 panel, select **Plugins**.
4. From the **Plugins** list, select **Fortify Remediation**.
5. In the **Fortify Remediation** panel on the right, click **Uninstall**.
6. In the **Fortify Remediation** panel 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.

To connect to Fortify Software Security Center and open an application version in the Fortify Remediation Plugin:

1. Open a project in the IDE.
2. Select **Fortify > Connect to Software Security Center**.
3. Type your Fortify Software Security Center credentials if prompted, and then click **OK**.

Note: If you are already connected to the Fortify Software Security Center, you do not need to re-type your credentials.

The Select Software Security Center Application Version dialog box opens and lists the existing applications and application versions.

4. Select an application version to work with, and then click **OK**.

The Fortify Remediation Plugin downloads the audit results from the Fortify Software Security Center application version.

Viewing Audit Results

Audit projects in the Fortify Remediation Plugin provide the security-related issues associated with a specific application. Audit projects organize these issues into folders based on filters.

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 in a project to quickly change issue sorting and visibility.

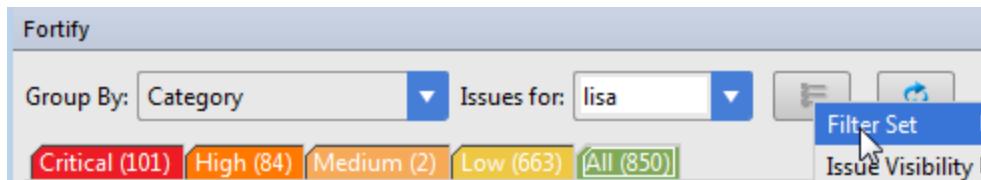
To remediate issues, the project you have open in the IDE must correspond to the application version you selected from Micro Focus Fortify Software Security Center when you connected to it from the Fortify Remediation Plugin. See "[Opening Fortify Software Security Center Application Versions](#)" on the previous page.

To update the audit results at any time with Fortify Software Security Center, click **Refresh** .

Grouping and Selecting Issues

When you connect to an application, the Fortify Remediation Plugin downloads the issues for that application version. Micro Focus Fortify Software Security Center provides several default folder types. Your view might be different, depending on whether your organization has created custom folders.

1. Click the **Change View Options**  icon.



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).
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 more information, see "[Grouping Issues](#)" below.
4. From the **Issues for** list, select one of the following:
 - **<All Users>**
 - Your Fortify Software Security Center user name.
 - Possibly additional Software Security Center user names
5. Click one of the following category tabs.
 - 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 have a 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.
6. Select a folder to view the associated issues.
The available folders are based on your **Group By**, **Issues for**, and **Filter Set** selections. At the end of 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. After you select a folder, the plugin retrieves the appropriate issues from Fortify Software Security Center.
7. Select an issue to view.

Grouping Issues

The items visible in the navigation tree vary depending on the selected grouping option. The value you select from the **Group By** list sorts issues in all visible folders into subfolders.

To list all issues in a folder without any grouping, select **<none>**.

You can view issues using any of the Group By options, and you can create and edit customized groups. The Group By options enable you to group and view the issues in different ways. In practice, you will

probably switch frequently between various groupings. The following table lists descriptions of the standard 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).
Analyzer	Groups issues by analyzer group, such as Control Flow, Data Flow, Findbugs, 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.
Correlated	Groups issues by whether the issue is related directly or indirectly with an issue uncovered by another analyzer.
Correlation Group	Groups issues that are correlated with each other.
File Name	Groups issues by file name.
Fortify Priority Order	Groups issues as Critical, High, Medium, and Low based on the analyzer's combined values of impact and likelihood.
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.
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.
<metadata_listname>	Groups issues using the alternative metadata external list names (for example, OWASP Top 10 <year>, CWE, PCI <version>, STIG <version>, and so on).

Option	Description
Package	Groups issues by package or namespace. Does not appear for projects for which this option is not applicable, such as C projects.
Sink	Groups issues that share the same dataflow sink function.
Source	Groups issues that share the same dataflow source functions.
Source File Type	Groups issues by source file types that Fortify Static Code Analyzer recognizes. Note: Issues in files with different file extensions that are the same source file type are grouped together (for example, issues in files with the extensions: html, htm, and xhtml are grouped under html).
Taint Flag	Groups issues by the taint flags that they contain.
<none>	Displays a flat view without grouping.

Viewing Issue Information

After you select an issue, the Fortify Remediation Plugin organizes issue-specific content and displays it on the **Audit**, **Recommendations**, **Details**, and **History** tabs, which are described in the following topics.

Audit Tab

The **Audit** tab provides a dashboard for selected issues. It includes a **User** list and an **Analysis** list, which you use to assign a user and analysis value to issues. The **Audit** tab also displays any custom tags defined for the Micro Focus Fortify Software Security Center application version.

This tab also displays an abstract of each issue, any comments that have been added, and an issue tree (Analysis Trace). You can click an issue in the Analysis Trace box to jump to its location in your code (if you have the same project open in the IDE as you selected from Fortify Software Security Center with the Fortify Remediation Plugin).

The method `execOptions()` in `Exec.java` calls `exec()` with a command built from untrusted data. This call can cause the program to execute malicious commands on behalf of an attacker.

```

    ↪() ParameterParser.java:627 - getParameterValues(return)
    := ParameterParser.java:627 - Assignment to values
    ↪() ParameterParser.java:638 - Return values[0]
    ↪() ParameterParser.java:608 - getRawParameter(return)
    ↪() ParameterParser.java:608 - Return
    ↪() Challenge2Screen.java:642 - getRawParameter(return)
    := Challenge2Screen.java:642 - Assignment to protocol
  
```

Recommendations Tab

The **Recommendations** tab contains 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	Recommendations for the selected issue type, and any custom recommendations defined by your organization
Tips/Custom Tips	Tips for the selected issue type, and any custom tips defined by your organization
References/Custom References	Reference information, including any custom reference defined by your organization

Details Tab

The **Details** tab provides a short abstract of the selected issue, detailed explanations, and examples with code samples. The following table describes the sections on this tab.

Section	Description
Abstract/Custom Abstract	Summary description of an issue, including custom abstracts defined by your organization

Section	Description
Explanation/Custom Explanation	Conditions in which the selected issue type occurs Discussion of the vulnerability, the constructs typically associated with it, ways in which attackers can exploit it, and the potential ramifications of an attack Any custom explanations defined by your organization
Instance ID	Unique identifier for an issue
Primary Rule ID	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 an issue

History Tab

The **History** tab displays the history of the selected issue, including changes made by the assigned user, the Analysis tag, and any custom tags.

Assigning Users to Issues

To assign a user to the issue:

1. Select an issue from the issues panel.
2. Select the **Audit** tab, and then, from the **User** list, select a user.
To leave the issue unassigned, select the blank value.

The Fortify Remediation Plugin communicates with Micro Focus Fortify Software Security Center and updates the project.

Assigning Tags to Issues

To assign tag values to an issue:

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

3. If custom tags defined for the project exist, provide values for them.

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

Adding Comments to Issues

You can use the Fortify Remediation Plugin to add comments to an issue.

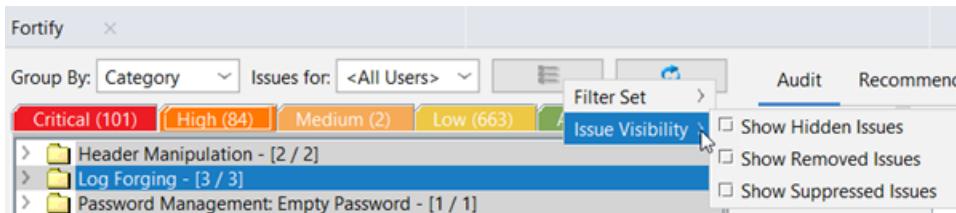
1. Select an issue from the issues panel.
2. From the **Audit** tab, click **Add Comment** .
3. In the Add Comment for Issue dialog box, type your comment.
4. Click **OK**.

The Fortify Remediation Plugin communicates with Micro Focus Fortify Software Security Center and updates the related project.

Customizing Issue Visibility

You can customize the issues view to determine which issues are displayed.

1. Click the **Change View Options**  icon.



2. From **Issue Visibility**, choose from the following options:
 - To display all hidden issues, select **Show Hidden Issues**.
 - To display all the issues removed since the previous analysis, select **Show Removed Issues**.
 - To display all suppressed issues, select **Show Suppressed Issues**.

The Fortify Remediation Plugin displays issues based on your selection.

Note: You can also change 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.
[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.
audited	Searches the issues to find true if the primary custom tag is set and false if the primary custom 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.

Modifier	Description
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.
file	Searches for issues where the primary location or sink node function call occurs in the specified file.
[fortify priority order]	<p>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 <i>impact</i> and <i>likelihood</i> of exploitation.</p> <p>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.</p>
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.

Modifier	Description
[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.
[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 .
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 (SCA, WebInspect, and 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.
minconf	Searches for all issues that have a confidence value equal to or greater than the number specified as the search term.

Modifier	Description
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.
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 and [source context] .
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] .
source	Searches for dataflow issues that have the specified source function name. Also see [source context] .

Modifier	Description
[source context]	<p>Searches for dataflow issues that have the source function call contained in the specified code context.</p> <p>Also see source and [primary context].</p>
sourcefile	<p>Searches for dataflow issues with the source function call that the specified file contains.</p> <p>Also see file.</p>
sourceline	<p>Searches for dataflow issues having taint source entering the flow on the specified line.</p>
status	<p>Searches issues that have the status reviewed, not reviewed, or under review.</p>
suppressed	<p>Searches for suppressed issues.</p>
taint	<p>Searches for issues that have the specified taint flag.</p>
trigger	<p>Searches for issues that contain the search term in the part of the response that shows that a vulnerability occurred for penetration test results.</p>
url	<p>Searches for issues based on the specified URL.</p>
user	<p>Searches for issues assigned to the specified user.</p>
<custom_tagname>	<p>Searches the specified custom tag.</p> <p>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).</p> <p>To search a date-type custom tag, specify the date in the format: yyyy-mm-dd.</p>
<metadata_Listname>	<p>Searches the specified metadata external list. For example, [owasp top 10 <year>], [cwe top 25 <year>], [pci CSS <version>], [stig <version>], and others.</p>

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:

1. Select an issue from the issues panel.

The Fortify Remediation Plugin communicates with Fortify Software Security Center and updates with the most recent project data. The focus jumps to the line of code that corresponds to the selected issue.

2. 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.

Troubleshooting the Remediation Plugin

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\IntelliJ.Plugin-<version>\log`

- On Linux and macOS:

`<userhome>/.fortify/IntelliJ.Plugin-<version>/log`

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on User Guide (Fortify Plugins for JetBrains IDEs 20.1.0)

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!