opentext™

OpenText™ Fortify Remediation Plugin for IntelliJ IDEA and Android Studio

Software Version: 24.2.0

User Guide

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 2012 - 2024 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks 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 September 24, 2024. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

Contents

Preface

Contacting 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 Product Documentation website:

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

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

https://community.microfocus.com/cyberres/fortify/w/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
24.2.0 / Revision 1: September 2024	Updated: • Added supported IDE versions (see "Requirements for Using the Fortify Remediation Plugin" on page 8) Removed: • Requirement that the Fortify Software Security Center version must correspond with the Fortify Remediation Plugin version
24.2.0	Added: • "Auditing Multiple Issues" on page 32 • "Suppressing Issues" on page 33 Updated: • Content added for overriding issue priority (see "Auditing Analysis Results" on page 30) • Changes made throughout the guide to reflect that the Fortify Remediation Plugin for IntelliJ IDEA and Android Studio commands are under the IDE **Tools** menu.
23.1.0	Updated: • Added support for custom tags that require comments (see "Auditing Analysis Results" on page 30)
22.2.0	This new document contains the Fortify Remediation Plugin for IntelliJ IDEA and Android Studio content that was previously covered in the *Micro Focus Fortify Plugins for JetBrains IDEs and Android Studio User Guide*. Added: • "Configuration Options" on page 33

Software Release / Document Version	Change
	Updated: • Added the Engine Priority grouping attribute (see "Grouping Issues" on page 14) • Added the `engine priority` search modifier (see "Search Modifiers" on page 18) • Added how to search for issues based on whether a custom tag is empty (see "Search Modifiers" on page 18)

Getting Started

This guide describes how to install the Fortify Remediation Plugin for IntelliJ IDEA and Android Studio (Fortify Remediation Plugin), and use it to review analysis results stored on an OpenText™ Fortify Software Security Center server.

About the Fortify Remediation Plugin

The Fortify Remediation Plugin works together with Fortify Software Security Center to add remediation functionality to your software security analysis. This plugin works with IntelliJ IDEA, Android Studio, PyCharm, and WebStorm, and more.

You can use the Fortify Remediation Plugin to:

- Review analysis results for applications in Fortify Software Security Center from within the IDE
- Audit the analysis results by assigning users or tags to issues, and adding comments to issues
- Fix and eliminate security issues in your code

Requirements for Using the Fortify Remediation Plugin

To use the Fortify Remediation Plugin, you must have the following:

- A Fortify Software Security Center URL
- Supported IntelliJ IDEA versions: 2022.x, 2023.x, 2024.1
- Supported Android Studio versions: 2022.x, 2023.x
- If your Fortify Software Security Center server uses an SSL connection from an internal certificate authority or a self-signed certificate, you must import the trusted certificate into the Java Runtime Environment (JRE) certificate store for the IDE. See the IDE documentation for more information. The following are examples of the certificate storage location for two IDEs:

  - IntelliJ IDEA: *<IDE_install_dir>*/jbr/lib/security/cacerts

  - Android Studio: *<IDE_install_dir>*/jre/lib/security/cacerts

- A user account on the Fortify Software Security Center server that has permission to access application versions

  To log into Fortify Software Security Center, you can use a user name and password or an authentication token.

- To audit issues in the analysis results, your user account must have audit permissions

  In addition to audit permissions, the following audit tasks require additional permissions:

  ○ To add comments to issues or assign values to custom tags that require comments, your user account must have the permission to comment on issues.

  ○ To override issue priority, your user account must have the permission to edit restricted custom tag values.

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

Installing the Fortify Remediation Plugin

You can install the Fortify Remediation Plugin on Windows, Linux, and macOS. Install the plugin directly from the **Marketplace** in the IDE settings.

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 **Settings** or **Preferences**.
3. In the left pane, select **Plugins**.
4. Select the **Marketplace** tab, and then in the search box type `Fortify Remediation`.
5. Select the Fortify Remediation Plugin, and then click **Install**.
6. Click **OK**.
7. To activate the plugin, restart the IDE.

The IDE **Tools** menu now includes the **Fortify** menu.

Related Documents

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

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

Fortify Software Security Center

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

Document / File Name	Description
OpenText™ 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 Fortify Software Security Center. It provides all the information you need to acquire, install, configure, and use Fortify Software Security Center. It is intended for use by system and instance administrators, database administrators (DBAs), enterprise security leads, development team managers, and developers. Fortify Software Security Center provides security team leads with a high-level overview of the history and status of a project.

Viewing Analysis Results

After you open an application version on Fortify Software Security Center, the Fortify Remediation Plugin displays the analysis results in a Fortify Remediation window. This window displays all security issues, organized in colored-coded tabs (folders) in an issue pane. Issues are organized based on settings in Fortify Software Security Center. To the right of the issue pane are four tabs that provide information specific to the issue selected in the issue pane.
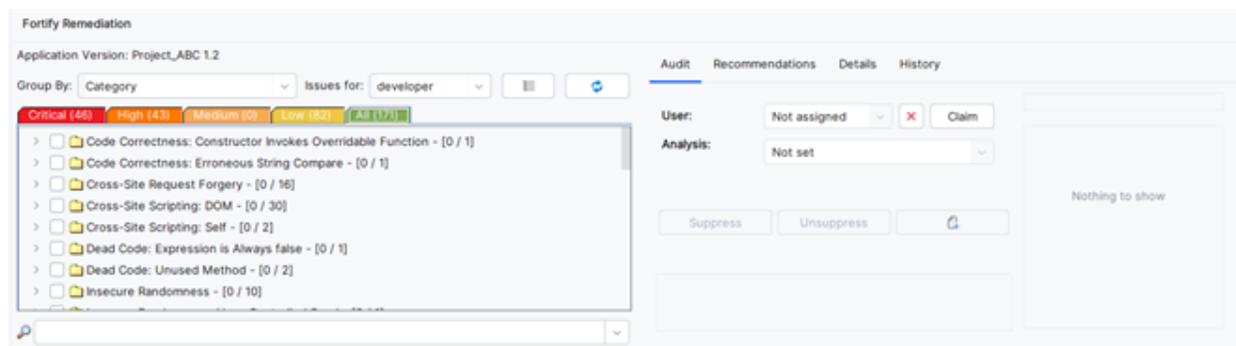
Color-coded tabs (folders) contain logically defined sets of issues. For example, the **Critical** folder contains all critical issues for a project. Similarly, the **Low** folder contains all low-priority issues. Filters determine which issues are visible. Filters are organized into distinct groups called filter sets. For information on applying filter sets, see "Viewing and Selecting Issues" on page 12.

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 a Fortify Software Security Center Application Version" below).

Opening a Fortify Software Security Center Application Version

To use the Fortify Remediation Plugin, you must first connect to Fortify Software Security Center and open an application version.

To open an application version in the Fortify Remediation Plugin:

1. Select **Tools > Fortify > Connect to Software Security Center**.

   The Software Security Center Credentials dialog box opens.
2. In the **SSC URL** box, specify the web address for your Fortify Software Security Center server.
3. From the **Login method** list, select the login method set up for you in Fortify Software Security Center.
4. Depending on the selected login method, use the procedure described in the following table.

Login Method	Procedure
Username/Password	Type your Fortify Software Security Center user name and password.
Authentication Token	In the **Token** box, specify the decoded value of a Fortify Software Security Center authentication token of type ToolsConnectToken. **Note:** For instructions on how to generate a Fortify Software Security Center authentication token, see the *OpenText™ Fortify Software Security Center User Guide*.

5. Click **OK** to connect to Fortify Software Security Center.

   The Select Software Security Center Application Version dialog box opens and displays the application versions that your user account has permission to access.
6. Select an application version to open, and then click **OK**.

The Fortify Remediation Plugin displays the analysis results for the selected application version on Fortify Software Security Center.

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

Viewing and Selecting Issues

To view and select issues in an opened application version:

1. Click the **Change View Options** button .
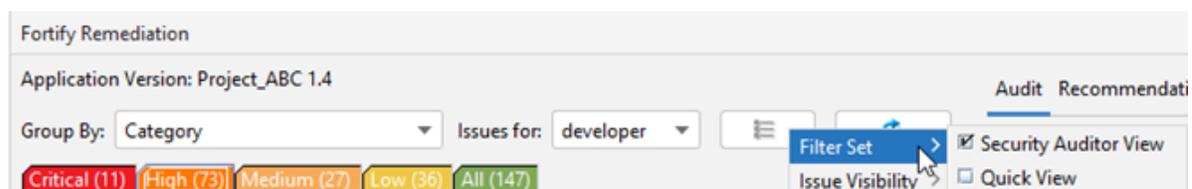
2. From **Filter Set**, select one of the following filter sets to apply to issues:
   - Select **Security Auditor View** to list all issues relevant to a security auditor.

   - 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 depend on the issue template assigned to the application version you opened.

3. From the **Group By** list, select an attribute for sorting issues in all visible folders into groups.

   The default grouping is **Category**. For a description of the available **Group By** attributes, see .

4. By default, issues assigned to your 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 depend on your **Filter Set**, **Group By**, and **Issues for** selections. It is possible that not all tabs are shown. The tabs shown also depend on the issue template associated with the application version.
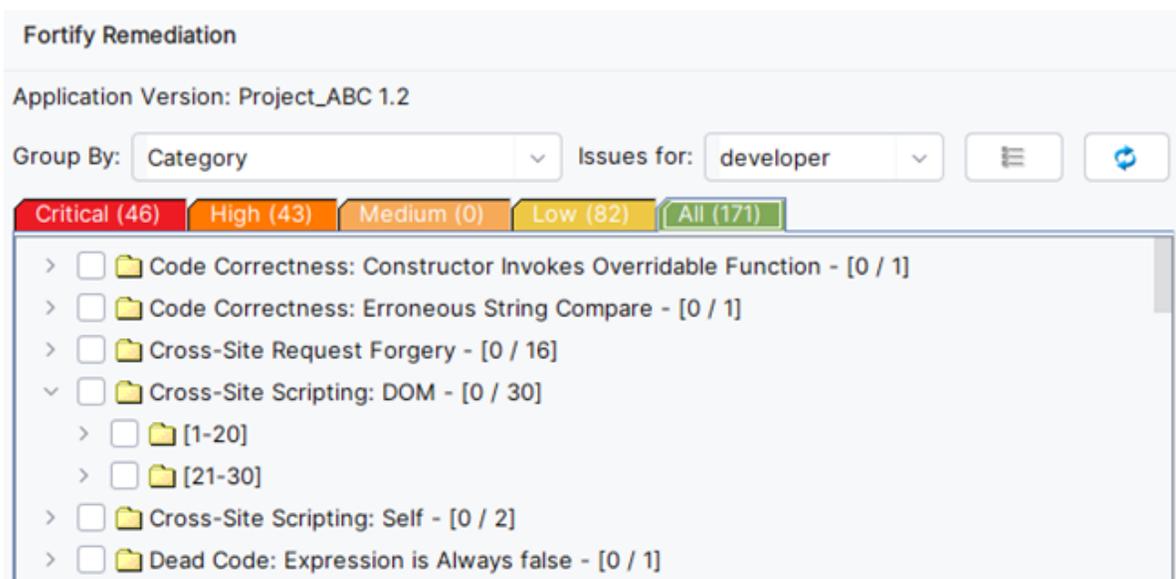
   - The **Critical** tab contains issues that have a high impact and a high likelihood of exploitation. Fortify recommends that you remediate critical issues immediately.

- 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 was audited.

6. Click to expand a folder and view the associated issues.

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

Fortify Remediation

Application Version: Project_ABC 1.2

Group By: Category ⌄   Issues for: developer ⌄   ☰   ⟳

Critical (46) | High (43) | Medium (0) | Low (82) | All (171)

- › ☐ 📁 Code Correctness: Constructor Invokes Overridable Function - [0 / 1]
- › ☐ 📁 Code Correctness: Erroneous String Compare - [0 / 1]
- › ☐ 📁 Cross-Site Request Forgery - [0 / 16]
- ⌄ ☐ 📁 Cross-Site Scripting: DOM - [0 / 30]
  - › ☐ 📁 [1-20]
  - › ☐ 📁 [21-30]
- › ☐ 📁 Cross-Site Scripting: Self - [0 / 2]
- › ☐ 📁 Dead Code: Expression is Always false - [0 / 1]

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 30 issues, the first 20 issues are in a subfolder labeled **[1-20]** and the last set of issues are in a subfolder labeled **[21-30]**. 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 how to set these properties, see "Configuration Options" on page 33.

7. To view the issue information for one issue, click an issue name.

The issue information is displayed in the **Audit** tab.

8. To select multiple issues so you can add the same audit information to them, select the check box for each issue.

    Switching to a different folder (tab) clears any previously selected issues.

    > **Tip:** Right-click an issue to clear all the selected issues or to select all issues in the current folder (tab).

    When you select more than one issue, the **Bulk Audit** tab is displayed.

See Also

"Grouping Issues" below

"Searching for Issues" on page 17

Grouping Issues

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

Issue Attribute	Description
Analysis	Groups issues by the audit analysis value assigned, such as Suspicious, Exploitable, and Not an Issue.
Analysis Type	Groups issues by analyzer product, such as SCA, WEBINSPECT, and SECURITYSCOPE (OpenText™ Fortify WebInspect Agent).
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 the selected custom tag.
Engine Priority	Groups issues based on the original priority value determined by the engine that identified the issue. **Note:** This is only available in Fortify Software Security Center version 22.2.0 or later.

| Issue Attribute	Description
File Name	Groups issues by file name.
Folder	Groups issues by folders defined in the issue template.
Fortify Priority Order	Groups issues by Critical, High, Medium, and Low based on the issue priority.
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 OpenText™ 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 are displayed 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. Nothing is shown for projects to which this option does not apply, such as C projects.
Primary Context	Groups issues where the primary location or sink node function call occurs in the same code context.
Priority Override	Groups issues by the Priority Override tag value assigned.
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

Issue Attribute	Description
	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 issue pane to determine which issues the Fortify Remediation Plugin displays.

To customize the issues pane:

1. Click the **Change View Options** button ▤ .
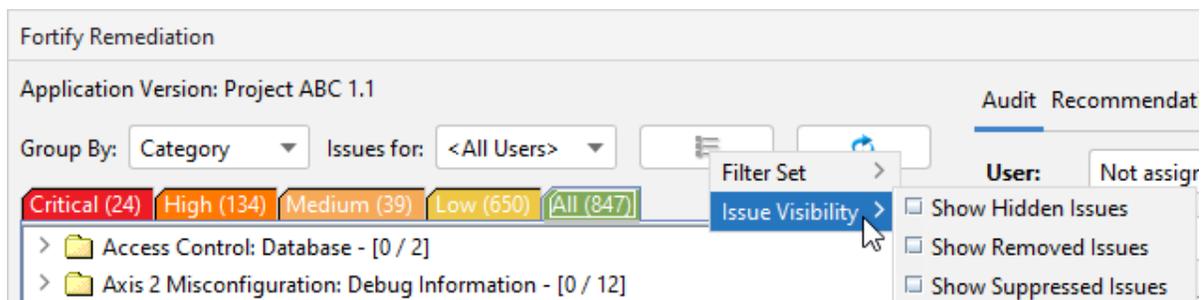
2. From the **Issue Visibility** list, select one of the following options:
   - To display all hidden issues, select **Show Hidden Issues**.

     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 **Tools > Fortify > Remediation Options**).

Searching for Issues

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

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

See Also

Search Syntax

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.

See Also

Search Modifiers

You can use a search modifier to specify to which issue attribute 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 matches the search string based 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.

The following examples describe using the search with and without applying a search modifier:

- 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 detected by the Control Flow Analyzer.

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

Search Modifier (Issue Attribute)	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 based on the 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.

Search Modifier (Issue Attribute)	Description
`[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 based on the intended audience, such as `dev`, `targeted`, `medium`, `broad`, and so on. **Caution!** This metadata is legacy information that is no longer used and will be removed in a future release. OpenText recommends that you not use this search modifier.
`audited`	Searches for issues based on whether the primary tag is set (`true` or `false`). 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 added to the issue.
`commentuser`	Searches for issues with comments from a specified user.
`confidence` (`con`)	Searches for issues that have the specified confidence value 0.1 through 5.0 (legacy metadata).
`cookies`	Searches for issues that contain the search term in the cookie from the HTTP query for penetration test results.

Search Modifier (Issue Attribute)	Description
`correlated`	Searches for issues based on whether the issues are correlated with those detected by 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 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 for a specific date in a date-type custom tag, specify the date in the format: yyyy-mm-dd. To search for issues that have no value set for a custom tag, use `<none>` as the search term. For example, to search for all issues that have no value set in the custom tag labeled Target Date, type: `[Target Date]:<none>`.
`[engine priority]`	Searches for issues based on the original priority value determined by the engine that identified the issue. **Note:** This is only available in Fortify Software Security Center version 22.2.0 or later.
`file`	Searches for issues where the primary location or sink node function call occurs in the specified file path.
`[fortify priority order]`	Searches for issues that have a priority level that matches the specified issue priority. Valid values are `critical`, `high`, `medium`, and `low`.
`headers`	Searches for issues that contain the search term in the request header for penetration test results.

Search Modifier (Issue Attribute)	Description
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.
[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 23.
manual	Searches for issues that were manually created by penetration test tools, and not automatically produced by a web crawler such as OpenText™ Fortify WebInspect.
[mapped category]	Searches for issues based on the specified category that is mapped across the various analyzers (OpenText™ 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.

Search Modifier (Issue Attribute)	Description
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).
method	Searches for issues based on the method, such as GET, POST, and so on.
minconf	Searches for all issues that have a confidence value equal to or greater than the number specified as the search term.
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" on the next page and "[source context]" on the next page.
primaryrule (rule)	Searches for all issues related to the specified sink rule.
[priority override]	Searches for all issues that have the specified Priority Override tag value. Valid values are critical, high, medium, and low.
probability	Searches for issues based on the probability value specified (1.0 through 5.0).

Search Modifier (Issue Attribute)	Description
[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]" on the previous page.
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 in the specified code context. Also see "source" above and "[primary context]" on the previous page.
sourcefile	Searches for dataflow issues with the source function call that the specified file contains. Also see file.
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

The following table contains search query examples.

| Search task	Search query
All privacy violations in file names that contain `jsp` with `getSSN()` as a source	`category:"privacy violation" source:getssn file:jsp`
All file names that contain `com/test/123`	`file:com/test/123`
All issues that contain `cleanse` as part of any modifier	`cleanse`
All suppressed vulnerabilities with `asdf` in the comments	`suppressed:true comments:asdf`
All categories except for SQL Injection	`category:!SQL Injection`
All issues that have a value specified for a custom tag labeled `version`	`version:!<none>`

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. If you select more than one issue, Fortify Remediation Plugin for Eclipse displays the **Bulk Audit** tab (see).

Audit Tabs

The **Audit** tab provides a dashboard of analysis information for a selected issue. Any changes you make on the **Audit** tab are automatically uploaded to the application version in Fortify Software Security Center.
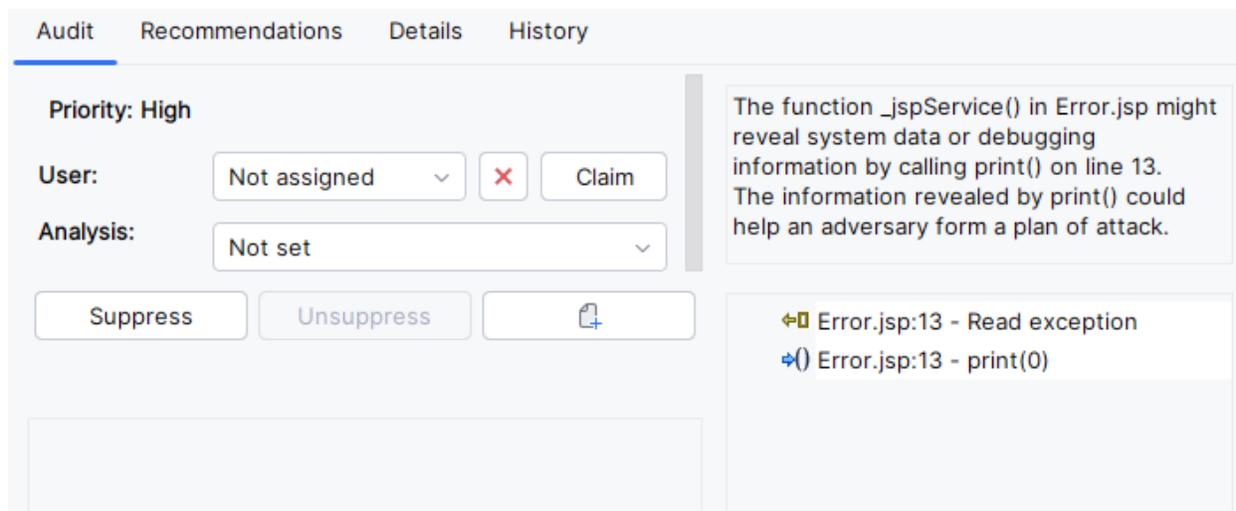
The **Bulk Audit** tab displays only the audit settings that you can apply to multiple selected issues. To apply any audit updates for multiple issues to Fortify Software Security Center, click **Save**.
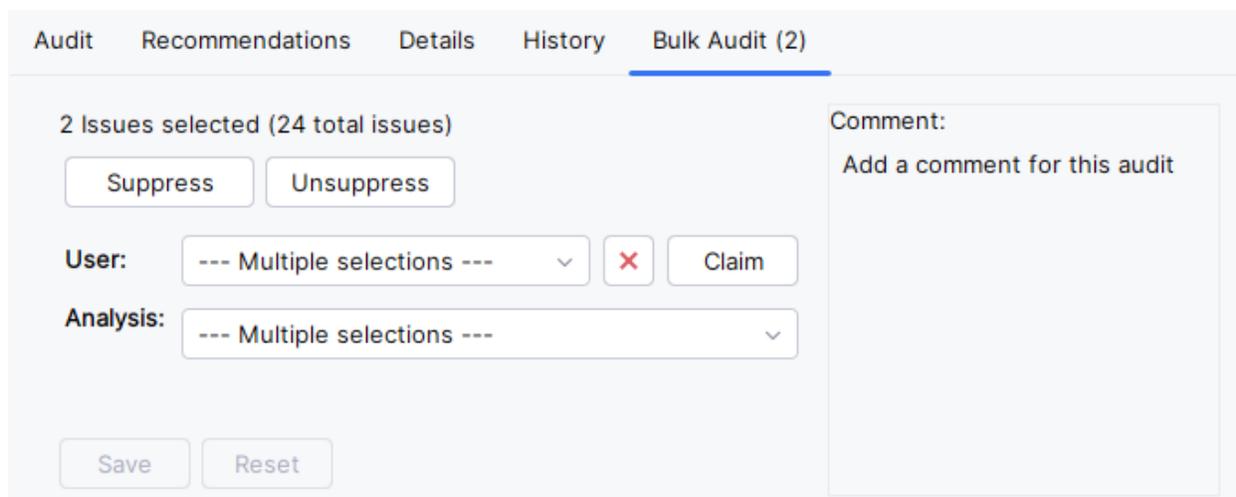
The following table describes features on the audit tabs.

Element	Description	Tab
User	The user assigned to the selected issue. If the box is empty, no user is assigned to the selected issue.	Audit Bulk Audit
Analysis	Your assessment of 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 version. The default primary tag is **Analysis**,	Audit Bulk Audit

Element	Description	Tab
	but your organization might have a different tag designated as the primary tag.	
<custom_tagname>	Any custom tags your organization has defined in Fortify Software Security Center. If available, these are displayed below the primary tag. If the audit results have been submitted to OpenText™ Fortify 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 Fortify Audit Assistant assigned to the issue. You cannot change this tag value. • **AA_Confidence**—Confidence level from Fortify Audit Assistant for the accuracy of its **AA_Prediction** value. You cannot change this tag value. • **AA_Training**—Whether to include or exclude the issue from Fortify Audit Assistant training. You can change this value. For more information about Fortify Audit Assistant, see the *OpenText™ Fortify Software Security Center User Guide*.	Audit Bulk Audit
Comments (bottom left)	Any additional information added to the issue.	Audit
Issue Abstract (top right)	A summary of the selected issue.	Audit
Analysis Trace (bottom right)	Items of evidence that the analyzer uncovered. The analysis trace evidence is presented in the order it was discovered. For descriptions of the analysis trace icons, see "Analysis Trace" on the next page.	Audit

See Also

"Auditing Analysis Results" on page 30

"Auditing Multiple Issues" on page 32

Analysis Trace

The analysis 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, if 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, web address, 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 one of the following: • 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

Icon	Description
←▯	Data is read from a global variable
↵	Tainted data is returned from a function
&	A pointer is created
✱	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
0II0I	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 (a box surrounds the induction trace).

The italics and the box distinguish the induction from a standard subtrace. 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 defined by your organization.
References/Custom References	Lists references for the recommendations provided, including any custom references defined by your organization.
Tips/Custom Tips	Provides useful information specific to the selected issue, and any custom tips defined by your organization.

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	Summary of the selected issue, including any custom abstracts defined by your organization.
Explanation/Custom Explanation	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 includes any custom explanations defined by your organization.
Instance ID	Unique identifier for the issue.
Primary Rule ID	Identifier for the primary rule used to uncover the issue.
Priority Metadata Values	Priority metadata values for this issue including impact and likelihood.
Legacy Priority Metadata Values	Legacy priority metadata values for the issue including severity and confidence.

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.

Locating Issues in your Source Code

You can use the Fortify Remediation Plugin to locate security-related issues in your code. You must have the same project open in the IDE as you opened from Fortify Software Security Center.

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

• Select an issue in the issue pane.

• From the **Audit** tab, select a line in the analysis trace box.

The IDE places the focus on the line of code that contains the selected security-related issue.

Auditing Analysis Results

After you select and review an issue, you can update the audit information on the **Audit** tab. To audit a batch of issues, see .To see any updates to the audit results made on Fortify Software Security Center, click the **Refresh** button .

To audit an issue:

1. From a folder in the issue pane, select an issue.
2. To assign a user to the selected issue, do one of the following:
   • Click **Claim** to assign the issue to yourself.

   • From the **User** list, select a user name.

   To remove an assigned user, click the **Unassign User** button .
3. From the **Analysis** list, select a value that reflects your assessment of this issue.

   This is the primary tag defined in Fortify Software Security Center. The default primary tag is **Analysis**, but it might be different for your organization.
4. If the priority override capability is enabled on Fortify Software Security Center, you can override the issue priority value by doing the following:
   a. From the **Priority Override** list, select the preferred priority value.
   b. Explain why you changed the value in the Add Comment for Issue dialog box.

   c. Click **OK**.

      The Priority changes to the value you selected. A warning symbol indicates that the Fortify-determined priority value was changed.
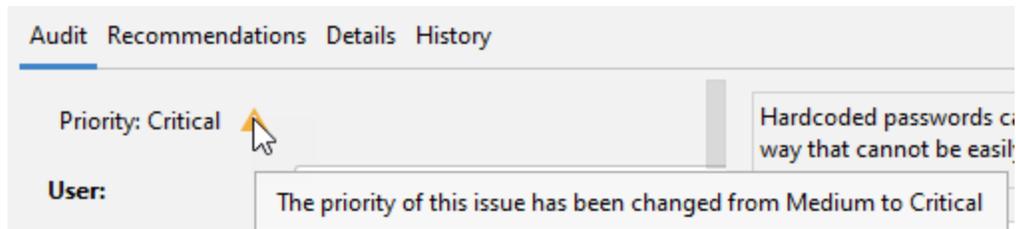
> **Note:** The issue is only visible in the newly assigned priority folder after the application metrics are refreshed on Fortify Software Security Center.

5. If additional custom tags are associated with the application version, specify values for those tags.

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

    Use the following information to provide values for custom tags:

- 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 the **Select Date** button ▤ to select a date from a calendar.

    If any tag requires a comment, then after you provide a value for the tag, the Add Comment for Issue dialog box opens. Type a comment to describe the value you specified for the tag, and then click **OK**.

> **Note:** If Fortify Audit Assistant assessed the issues, the following tags are shown **AA_Prediction**, **AA_Confidence**, and **AA_Training**. For information about these tags, see "Audit Tabs" on page 24.

6. To add a comment for the issue audit:

   a. Click the **Add Comment** button ▦ .

   b. In the Add Comment for Issue dialog box, type your comment, and then click **OK**.

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

See Also

"Auditing Multiple Issues" on the next page

"Suppressing Issues" on page 33

Auditing Multiple Issues

You can evaluate and assign audit information to a batch of issues. To audit a single issue on the **Audit** tab, see "Auditing Analysis Results" on page 30. To see any updates to the audit information made in Fortify Software Security Center, click the **Refresh** button ⟳.

To audit multiple issues:

1. From the issue list in the Remediation View, select multiple issues.
2. To assign a user to the selected issues, do one of the following:
   - Click **Claim** to assign the issues to yourself.
   - From the **User** list, select a user name.

   To remove an assigned user, click the **Unassign User** button ☒.
3. From the **Analysis** list, select a value that reflects your assessment of this issue.

   This is the primary tag defined in Fortify Software Security Center. The default name of this tag is **Analysis**, but it might be different for your organization.
4. If the priority override capability is enabled on Fortify Software Security Center, you can override the issue priority value by doing the following:
   a. From the **Priority Override** list, select the preferred priority value.
   b. Explain why you changed the value in the Add Comment for Issue dialog box.

   > **Note:** The issues are only visible in the newly assigned priority folder after the application metrics are refreshed on Fortify Software Security Center.

5. If additional custom tags are associated with the application version, specify values for those tags.

   The Fortify Remediation Plugin displays all custom tags assigned to the application, but you can only provide values for tags that your Fortify Software Security Center user account has permission to edit. Use the following information to provide values for custom tags:
   - 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 the **Select Date** button ▦ to select a date from a calendar.

   If any tag requires a comment, then after you provide a value for the tag, the Add Comment for Issue dialog box opens. Type a comment to describe the value you specified for the tag, and then click **OK**.

   > **Note:** If Fortify Audit Assistant assessed the issues, the following tags are shown **AA_Prediction**, **AA_Confidence**, and **AA_Training**. For information about these tags, see "Audit Tabs" on page 24.

6. To add a comment for the audit of these issues, type your comment in the **Comment** box.

7. Click **Save**.

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

See Also

"Suppressing Issues" below

"Auditing Analysis Results" on page 30

Suppressing Issues

You can suppress issues that are either fixed or that you do not plan to fix. Suppression marks the issue and all future discoveries of this issue as suppressed. As such, it is a semi-permanent marking of a vulnerability.

To suppress issues:

1. From the issue list in the Remediation View, select one or more issues.

2. On the **Audit** or **Bulk Audit** tab, click **Suppress**.

3. (Optional) In the Suppress Issue dialog box, describe the reason for suppressing the issue.

4. Click **OK** to confirm the issue suppression.

To unsuppress issues:

1. Make sure that suppressed issues are visible.

   To display issues that have been suppressed, see "Customizing Issue Visibility" on page 16.

2. From the issue list in the Remediation View, select one or more suppressed issues.

3. On the **Audit** or **Bulk Audit** tab, click **Unsuppress**.

4. (Optional) In the Unsuppress Issue dialog box, describe the reason for unsuppressing the issue.

5. Click **OK** to confirm the issue unsuppression.

Configuration Options

This topic describes the options you can configure for the Fortify Remediation Plugin. The options are stored as properties in a plain text file with the name `fortify.properties`. In this file, each property consists of a pair of strings: the first string is the property name and the second string is the property value. For example, the following sets the pagination count to 40:

```
com.fortify.remediation.PaginationCount=40
```

To specify any of these properties:

1. Navigate to the `<IDE_product_plugins_dir>/Fortify/config/` directory.
   The following is an example location on Windows:

```
C:\Users\jsmith\AppData\Roaming\JetBrains\IdeaIC2022.1\plugins\Fortify\
config
```

2. If the file does not already exist, use a text editor to create a `fortify.properties` file.

The following table describes the properties that you can set in the `fortify.properties` file.

Property	Description

com.fortify.AuthenticationKey	Specifies the directory used to store the encrypted Fortify Software Security Center authentication token.
	
	Default:
	`${com.fortify.WorkingDirectory}/config/IntelliJRemediation-`
	`<version>`

com.fortify.InstallationUserName	Specifies the default user name for logging in to Fortify Software Security Center for the first time. **Default:** `${user.name}`
com.fortify.remediation.PaginateIssues	If set to `true` or if no value is specified, the Fortify Remediation Plugin uses pagination during issue download. If set to `false`, the Fortify Remediation Plugin downloads all the issues at once. **Default:** `true`
com.fortify.remediation.PaginationCount	If `com.fortify.remediation.PaginateIssues` is set to `true`, specifies the number of issues to display per subfolder. **Default:** `20`
com.fortify.WorkingDirectory	Specifies the working directory that contains all user configuration and working files for the plugin. To configure this property, you must have write permission in the directory. **Defaults:** • Windows—`${win32.LocalAppdata}/Fortify` • Non-Windows—`${user.home}/.fortify`

Locating Log Files

For help diagnosing a problem with the Fortify Remediation Plugin, provide the log file to Fortify Software Security Center. 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 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 Remediation Plugin for IntelliJ IDEA and Android Studio 24.2.0)

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@opentext.com.

We appreciate your feedback!