Micro Focus Fortify Remediation Plugin for Eclipse

Software Version: 23.1.0

User Guide

Document Release Date: June 2023
Software Release Date: June 2023

MICRO FOCUS®

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 2013 - 2023 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 May 31, 2023. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

Contents

Preface

Contacting Micro Focus Fortify Customer Support

Visit the Support website to:

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

https://www.microfocus.com/support

For More Information

For more information about Fortify software products:

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

About the Documentation Set

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

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

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

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

Fortify Product Feature Videos

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

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

Change Log

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

Software Release / Document Version	Change
23.1.0	Updated: • Added that you can install the Fortify Remediation Plugin for Eclipse from the Eclipse Marketplace (see "Installing the Fortify Remediation Plugin for Eclipse" on page 8) • Added support for custom tags that require comments (see "Assigning Tags to Issues" on page 30)
22.2.0	This new document contains the Fortify Remediation Plugin for Eclipse content that was previously covered in the *Micro Focus Fortify Plugins for Eclipse User Guide*. Added: • "Configuration Options" on page 33 Updated: • Added the Engine Priority grouping attribute (see "Grouping Issues" on page 14) • Added the `engine priority` search modifier (see "Search Modifiers" on page 17) • Added how to search for issues based on whether a custom tag is empty (see "Search Modifiers" on page 17)

Getting Started

This guide describes how to install the Fortify Remediation Plugin for Eclipse and use it to review analysis results stored on a Fortify Software Security Center server.

This section contains the following topics:

About the Fortify Remediation Plugin for Eclipse

The Fortify Remediation Plugin for Eclipse works together with Fortify Software Security Center to add remediation functionality to your software security analysis. The Fortify Remediation Plugin for Eclipse is a lightweight plugin option for developers who do not need the scanning and auditing capabilities of Fortify Audit Workbench and the Fortify Complete Plugin for Eclipse.

You can use the Fortify Remediation Plugin for Eclipse to:

- Review analysis results for applications in Fortify Software Security Center from within Eclipse
- 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 for Eclipse

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

- A Fortify Software Security Center URL

  The Fortify Software Security Center version must correspond with the Fortify Remediation Plugin for Eclipse version. The version number format is *<major>.<minor>.<patch>* (for example, 23.1.0). The *<major>* and *<minor>* portions of the Fortify Software Security Center and the Fortify Remediation Plugin for Eclipse version numbers must match. For example, versions 23.1.0 and 23.1.1 correspond.

- To use HTTPS to communicate with Fortify Software Security Center, you must import a self- or locally-signed certificate into the Java Runtime certificate store.
- 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
- To add comments to issues or assign custom tags that require comments, your user account must have the permission to comment on issues

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

Installing the Fortify Remediation Plugin for Eclipse

You can install the Fortify Remediation Plugin for Eclipse on Windows, Linux, and macOS. The following instructions describe how to install the Fortify Remediation Plugin for Eclipse from a Fortify server. Alternatively, you can install it using the Eclipse Marketplace Client.

To update from an earlier Fortify Remediation Plugin for Eclipse version, you must first remove the existing version. For information about how to uninstall the plugin, see "Uninstalling the Fortify Remediation Plugin for Eclipse from Eclipse" on the next page.

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 for Eclipse:

1. From Eclipse, select **Help > Install New Software**.
2. Click **Add**.

   The Add Repository dialog box opens.
3. (Optional) In the **Name** box, type a name for the update site.
4. In the **Location** box, type `https://tools.fortify.com/ssceclipseplugin`.
5. Click **Add**.

   On the **Available Software** step, the **Fortify Eclipse Remediation Plugin** node is listed as available software.
6. Click **Select All** and then click **Next**.
7. To see the version and copyright information for the plugin in the **Details** box, click the plugin name.
8. Click **Next**.
9. Click **Finish**.
10. To complete the installation and restart Eclipse, click **Restart Now** when prompted.

After Eclipse restarts, the menu bar displays the **Fortify** menu.

Uninstalling the Fortify Remediation Plugin for Eclipse from Eclipse

> **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 for Eclipse:

1. Start Eclipse.
2. Select **Help > About Eclipse IDE**, and then click **Installation Details**.
3. On the **Installed Software** tab, select **Fortify Remediation Plugin for Eclipse**.
4. Click **Uninstall**.
5. In the Uninstall window, click **Finish**.
6. To implement the change, click **Yes** to restart Eclipse.

The Eclipse menu bar no longer includes the **Fortify** menu.

Related Documents

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

> **Note:** You can find the Fortify Product Documentation at https://www.microfocus.com/support/documentation.

Fortify Software Security Center

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

Document / File Name	Description
Fortify Software Security Center User Guide SSC_Guide_*<version>*.pdf	This document provides Fortify Software Security Center users with detailed information about how to deploy and use Software Security Center. It provides all of the information you need to acquire, install, configure, and use Software

Document / File Name	Description
	Security Center.
	It is intended for use by system and instance administrators, database administrators (DBAs), enterprise security leads, development team managers, and developers. Software Security Center provides security team leads with a high-level overview of the history and current status of a project.

Viewing Analysis Results

After you open an application version on Fortify Software Security Center, the Fortify Remediation Plugin for Eclipse displays the analysis results in the **Remediation View**. This view displays all security issues, organized in color-coded tabs (folders) in an issue pane. Issues are organized based on the 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.
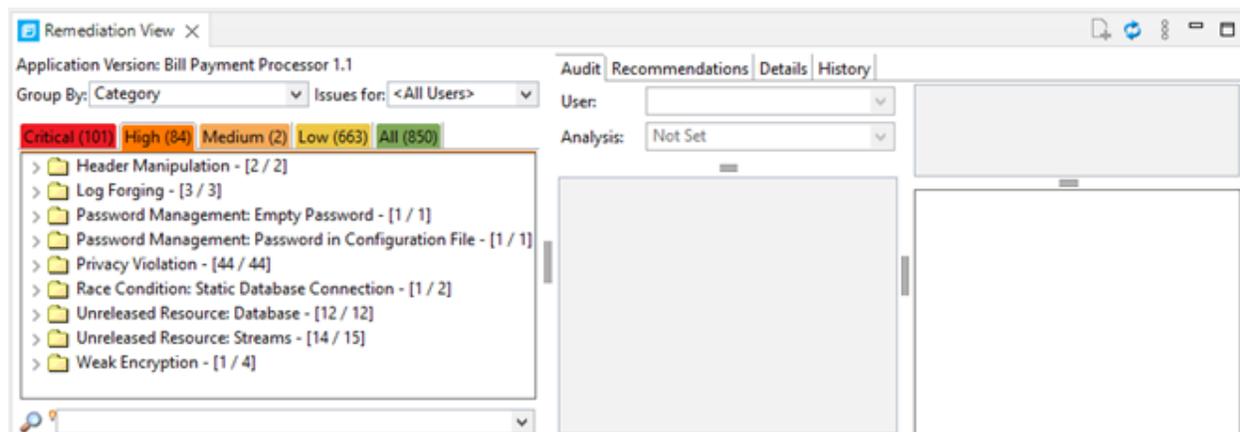
Color-coded tabs (folders) contain logically defined sets of issues. For example, the **Critical** folder contains all critical issues for a project. Similarly, the **Low** folder contains all low-priority issues. Filters determine which issues are visible. Filters are organized into distinct groups 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 Eclipse must correspond to the application version you opened in Fortify Software Security Center (see "Opening a Fortify Software Security Center Application Version" on the next page).

Opening a Fortify Software Security Center Application Version

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

> **Note:** The Fortify Software Security Center server that you connect to from the Fortify Remediation Plugin for Eclipse must be running continuously during your work session in Eclipse.

To open an application version in the Fortify Remediation Plugin for Eclipse:

1. Select **Fortify > Connect to Software Security Center**.
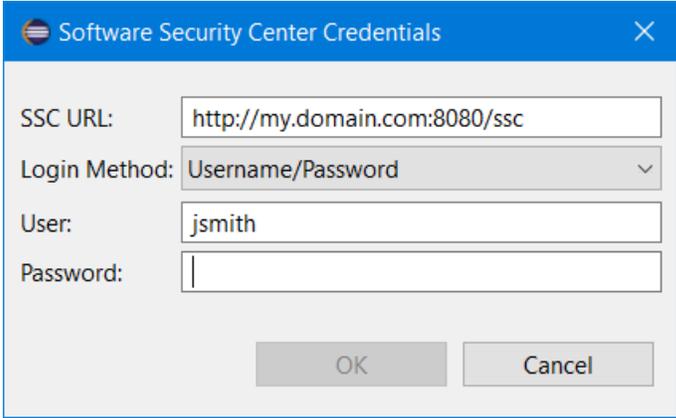
2. In the **SSC URL** box, specify the URL for your Fortify Software Security Center server.
3. From the **Login Method** list, select the login method set up for you on Fortify Software Security Center.
4. Depending on the selected login method, do one of the following:

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 about how to generate a Fortify Software Security Center authentication token, see the *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 for Eclipse 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 **Fortify > Open Application Version**. To switch to a different Fortify Software Security Center server, select **Fortify > Disconnect from Software Security Center** and then reconnect to Fortify Software Security Center as described in this topic.

Viewing and Selecting Issues

To view and select issues in an opened application version:

1. 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 "Grouping Issues" on page 14.

2. By default, issues for 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

3. To specify a filter set to apply to the issues, click the **View Menu** icon and then select **Filter Set > <filter_set_name>**.
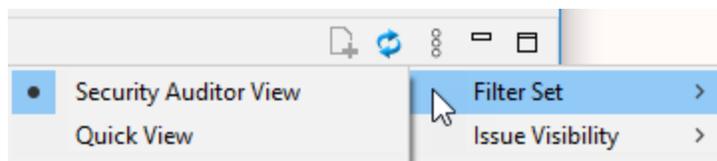
> **Note:** The filter sets available depends on the issue template assigned to the application version you opened.

4. Click a color-coded folder (tab) to view the associated issues.

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

   - The **Critical** folder contains issues that have a high impact and a high likelihood of exploitation. Remediate critical issues immediately.

- The **High** folder contains issues that have a high impact and a low likelihood of exploitation. Remediate these issues with the next patch release.

- The **Medium** folder contains issues that have a low impact and a high likelihood of exploitation. Remediate these issues as time permits.

- The **Low** folder contains issues that have a low impact and a low likelihood of exploitation. Remediate these issues as time permits.

- The **All** folder lists all issues.

Within each color-coded folder, issues are grouped into subfolders. 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 - [2 / 2]** indicates that two out of two issues categorized as Command Injection are audited.

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

The Fortify Remediation Plugin for Eclipse retrieves the corresponding issues from Fortify Software Security Center.
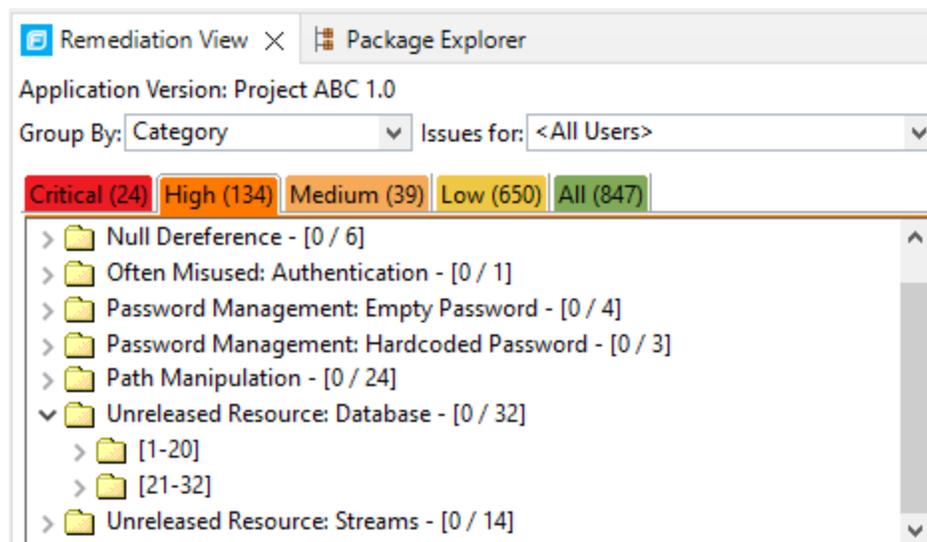
Note: By default, if a folder contains more than 20 issues, the issues are grouped into subfolders in blocks of 20 with folder names that indicate the issues included. For example, if a folder contains 32 issues, the first 20 issues are in a subfolder labeled **[1- 20]** and the last set of issues are in a subfolder labeled **[21-32]**. To change the default pagination setting of 20, set the `com.fortify.remediation.PaginationCount` property. You can also disable issue pagination by setting the `com.fortify.remediation.PaginateIssues` property to `false`. For more information about these properties, see the "Configuration Options" on page 33.

6. Select an issue to view its details.

For information about how to search for issues, see "Searching for Issues" on page 16.

Grouping Issues

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

Attribute	Description
Analysis	Groups issues by the audit analysis assigned, 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, 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 grouping.
<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.
File Name	Groups issues by file name.
Folder	Groups issues by folders defined in the issue template.
Fortify Priority Order	Groups issues as Critical, High, Medium, and Low based on the issue priority.
Introduced date	Groups issues by the date the issue was first detected.

Attribute	Description
Issue State	Groups audited issues by whether the issue is an open issue or not an issue based on the level of analysis set for the primary tag. Values equivalent to Suspicious and Exploitable are considered open issue states.
Kingdom	Groups issues by the Seven Pernicious Kingdoms classification.
Manual	Groups issues by whether they were manually created by penetration test tools, and not automatically produced by a web crawler such as Fortify WebInspect.
<metadata_listname>	Groups issues using the alternative metadata external list names (for example, OWASP Top 10 *<year>*, CWE, PCI SSF *<version>*, STIG *<version>*, and others).
New Issue	Shows which issues are new since the last scan. For example, if you run a new scan, any issues that are new 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.
Sink	Groups issues that share the same dataflow sink function.
Source	Groups issues that share the same dataflow source functions.
Source Context	Groups dataflow issues that have the source function call contained in the same code context.
Source File	Groups dataflow issues by the source code file where the taint originated.
Status	Groups issues by the audit status (**Reviewed**, **Unreviewed**, or **Under Review**).
Taint Flag	Groups issues by the taint flags that they contain.
URL	Groups dynamic issues by the request URL.

Customizing Issue Visibility

You can customize the issues list to determine which issues the **Remediation View** displays.

On the top right of the **Remediation View**, click the **View Menu** icon, select **Issue Visibility**, and then select whether to show hidden, removed, or suppressed issues.
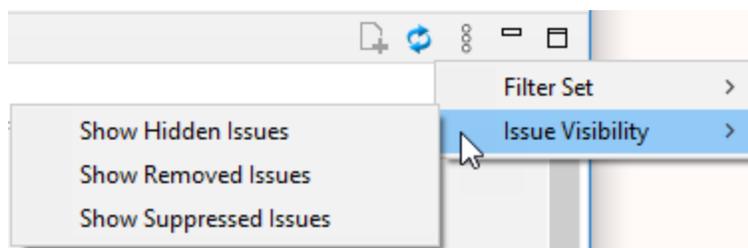
Select (or deselect) one of the following options:

- To display all issues that are excluded from display by visibility filters in filter sets such as the Quick View filter sets, 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 that were uncovered in the previous scan but are no longer evident in the most recent analysis results, select **Show Removed Issues**.

- To display all issues marked as suppressed (either because they are not of high priority or of immediate concern), 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.

Searching for Issues

You can use the search box below the issues list to search for issues. After you perform a search, the label next to the folder name changes to indicate the number of issues that match the search as a subset of the total.

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

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 (" ")

Comparison	Description
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 for using a modifier is `modifier:<search_term>`.

A search query can contain multiple modifiers and search terms. 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 query, 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" below

"Search Query Examples" on page 23

"Performing Searches" on page 23

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 matches the search query based on the following attributes: kingdom, primary rule id, analyzer, filename, severity, class name, function name, instance id, package, confidence, type, subtype, taint flags, category, sink, and source.

- To apply the search to all modifiers, type a string such as `control flow`. This searches all the modifiers and returns any results that contain the "control flow" 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 string.

Search 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 based on 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 based on intended audience such as `dev`, `targeted`, `medium`, `broad`, and so on. **Note:** This metadata is legacy information that is no longer used and will be removed in a future release. Fortify recommends that you 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.

Search 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 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.
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.

Search Modifier	Description
	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.
`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 `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 22.

Search Modifier	Description
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 Fortify WebInspect.
[mapped category]	Searches for issues based on the specified category that is mapped across the various analyzers (Fortify Static Code Analyzer, Fortify WebInspect, and Fortify WebInspect Agent).
maxconf	Searches for all issues that have a confidence value equal to or less than the number specified as the search term.
maxVirtConf	Searches for dataflow issues that have a virtual call confidence value equal to or less than the number specified as the search term.
<metadata_listname>	Searches for issues based on the value of the specified metadata external list. Metadata external lists include [owasp top ten *<year>*], [cwe top 25 *<version>*], [pci ssf *<version>*], [stig *<version>*], and others.
method	Searches for issues based on the method, such as GET, POST, DELETE, 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.

Search Modifier	Description
[primary context]	Searches for issues where the primary location or sink node function call occurs in the specified code context. Also see "sink" below and "[source context]" below.
primaryrule (rule)	Searches for all issues related to the specified sink rule.
probability	Searches for issues based on the probability value specified (1.0 through 5.0).
[remediation effort]	Searches for issues based on the remediation effort value specified. The valid values are whole numbers from 1.0 to 12.0.
response	Searches for issues that contain the search term in the response from the protocol used in penetration test results.
severity (sev)	Searches for issues based on the specified severity value (legacy metadata).
sink	Searches for issues that have the specified sink function name. Also see "[primary context]" above.
source	Searches for dataflow issues that have the specified source function name. Also see "[source context]" below.
[source context]	Searches for dataflow issues that have the source function call in the specified code context. Also see "source" above and "[primary context]" above.
sourcefile	Searches for dataflow issues with the source function call that the specified file contains. Also see "file" on page 20.
sourceline	Searches for dataflow issues having taint source entering the flow on the specified line. Also see "line" on page 20.
status	Searches issues that have the status reviewed, not reviewed, or under review.
suppressed	Searches for issues based on whether they are suppressed.
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

Search Modifier	Description
	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.

To search for...	Type...
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>`

Performing Searches

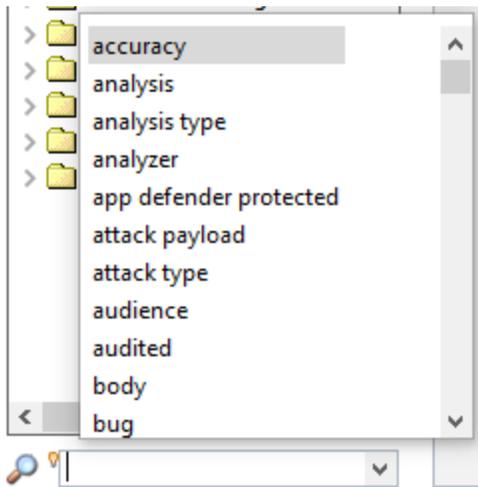To perform a simple search, do one of the following:

- Type a search query in the search box, and then press **Enter**.

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

To get assistance to compose a search query, do the following:

1. Click in the search box, and then press **Ctrl** + **Space**.

2. From the displayed list, double-click a search modifier to begin your search query.

3. For assistance to specify the comparison, with your cursor placed after the modifier in the search box, press **Ctrl** + **Space**.
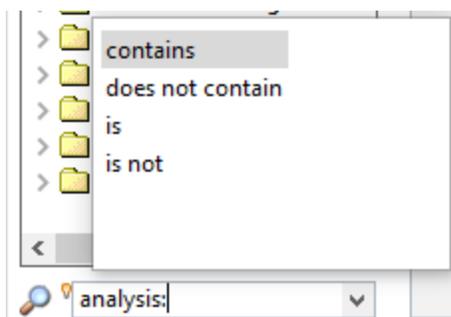
4. From the displayed list, double-click a comparison to add it to your search query.

5. Type the rest of the search query, and then press **Enter** to perform the search.
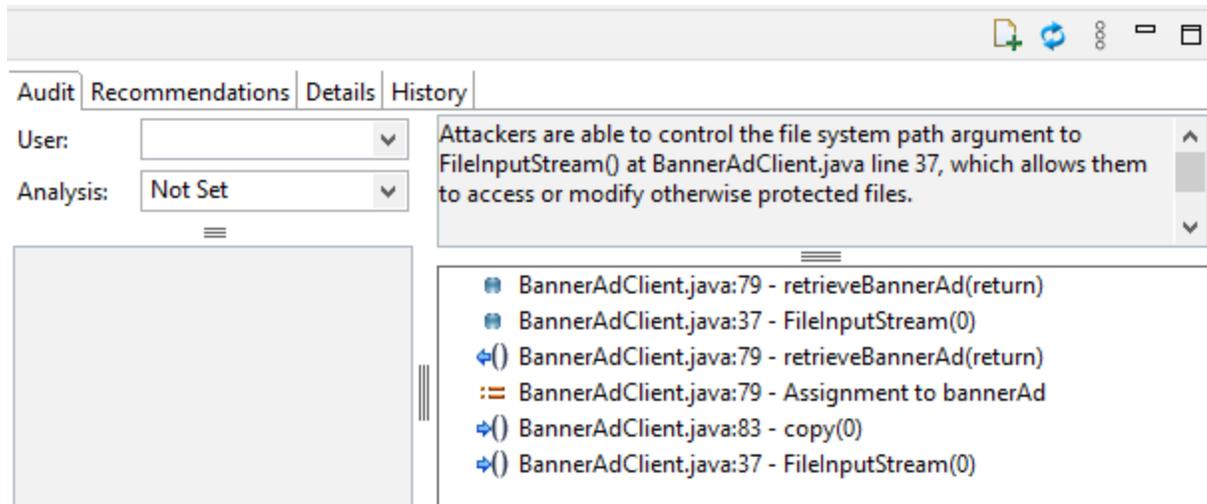
Viewing Issue Information

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

Audit Tab

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

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

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

Element	Description
User	The user assigned to the selected issue. If the box is empty, no user is assigned to the selected issue. For instructions on how to assign a user to an issue, see "Assigning Users to Issues" on page 30.
Analysis	Your assessment for the selected issue. To change the assessment, select an item from the list. This is the primary tag as defined in Fortify Software Security Center for the application version. The default primary tag is **Analysis**, 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. These are displayed below the primary tag. For information on how to make changes to these tags, see "Assigning Tags to Issues" on page 30.
	If the audit results have been submitted to Fortify Audit Assistant in Fortify Software Security Center, then in addition to any other custom tags, the tab displays the following tags:

Element	Description
	• **AA_Prediction**—Exploitability level that Fortify Audit Assistant assigned to the issue. You cannot modify this tag value. • **AA_Confidence**—Confidence level from Fortify Audit Assistant for the accuracy of its **AA_Prediction** value. This is a percentage expressed in values that range from 0.000 to 1.000. For example, a value of 0.982 indicates a confidence level of 98.2 percent. You cannot modify this tag value. • **AA_Training**—Whether to include or exclude the issue from Fortify Audit Assistant training. You can modify this value. For more information about Audit Assistant, see the *Fortify Software Security Center User Guide*.
Comments (bottom left)	Any additional information added to the issue. For instructions on how to add comments, see "Adding Comments to Issues" on page 31.
Issue Abstract (top right)	A summary of the selected issue.
Analysis Trace (bottom right)	The items of evidence that the analyzer uncovered. The analysis trace is presented in the order it was discovered. For information about the Analysis Trace icons, see "Analysis Trace" below.

See Also

"Adding Audit Information" on page 30

Analysis Trace

When you select an issue, the **Audit** tab displays the relevant analysis trace. This is a set of program points that show how the analyzer found the issue. For dataflow and control flow issues, the set is presented in the order executed. For dataflow issues, this trace view presents the path that the tainted data follows from the source function to the sink function. For example, when you select an issue that is related to potentially tainted dataflow, the analysis trace box shows the direction the dataflow moves 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 such as an HTML form or a URL
ⓖ	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 place 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
⇤▢	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

Icon	Description
	The execution jumps
	A branch is taken in the code execution
	A branch is not taken in the code execution
	Generic
01101	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.
Tips/Custom Tips	Provides useful information specific to the selected issue, and any custom tips defined by your organization.
References/Custom References	Lists references for the recommendations provided, including any custom references 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 for Eclipse to locate security-related issues in your code.

To jump to the line of source code that contains the issue selected in the Fortify Remediation Plugin for Eclipse:

1. Make sure that the revision of the source code open in Eclipse corresponds to the application version you opened on Fortify Software Security Center.

> **Note:** If the name of the Eclipse project and the Fortify Software Security Center application name are not the same, then the current open project in Eclipse is used. If you have multiple projects open in Eclipse, then you are prompted to select a project to use for the source code navigation.

2. Select an issue in the issue pane or select a line in the analysis trace box.

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

Adding Audit Information

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

Assigning Users to Issues

To assign a user to an issue:

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

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

The Fortify Remediation Plugin for Eclipse makes the update to the application version in Fortify Software Security Center.

Assigning Tags to Issues

To assign custom tag values to an issue:

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

    This is the primary tag as defined in Fortify Software Security Center. The default primary tag is **Analysis**, but your organization might have a different tag designated as the primary tag.

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

> **Note:** The Fortify Remediation Plugin for Eclipse 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.

For text-type custom tags, you can click **Edit Text** (   ) to see and edit long text strings. This tag accepts up to 500 characters (HTML/XML tags and newlines are not allowed).

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

4. If a 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**.

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

Adding Comments to Issues

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

To add a comment to an issue:

1. From a folder in the issue pane, select an issue.

2. At the top right of the **Remediation View**, click **Add Comment** (   ).

   The Add Comment for Issue dialog box opens.

3. In the Add Comment for Issue dialog box, type your comment

4. Click **OK**.

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

Generating and Downloading Reports

You can generate reports in Fortify Software Security Center from the Fortify Remediation Plugin for Eclipse. You can also download a report that has already been created in Fortify Software Security Center.

To generate or download a report, you must be connected to Fortify Software Security Center and have an application version opened. You are prompted to login to Fortify Software Security Center and select an application version if you have not done so (see "Opening a Fortify Software Security Center Application Version" on page 11.

Generating Reports

To generate a report:

1. Select **Fortify > Generate Report**.
2. If prompted, provide your Fortify Software Security Center credentials.

   Your user account must have permission to generate reports.
3. Select an application version and then click **OK**.

   The Software Security Center Report Generation dialog box opens.
4. Select a report type from the list.
5. Select the template version and the options you want to include in the report.

   > **Note:** The template version and options vary depending on the report type selected.

6. To specify the file name for the report and select the report format, click **Report details**.

   You can save the report in the following formats: Portable Document Format (PDF), Microsoft Word, and Microsoft Excel. The default report format is PDF.
7. Click **Generate**.
8. Navigate to where you want to save the report and click **Save**.

The report is generated and saved in the format you selected.

Downloading Reports from Fortify Software Security Center

To download a report that has been created in Fortify Software Security Center:

1. Select **Fortify > Download Generated Report**.
2. If prompted, provide your Fortify Software Security Center credentials.
3. Select the application version from which you want to download the report.
4. Select the report you want to download from the list of reports previously generated in Fortify Software Security Center.
5. Click **Download Report**.
6. Navigate to where you want to save the report and click **Save**.

Configuration Options

This topic describes the options you can configure for the Fortify Remediation Plugin for Eclipse. 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 property sets the pagination count to 40:

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

To specify any of these properties:

1. Navigate to one of the following directories:
   - If the Eclipse IDE was installed with an installer:

     <userhome>/.p2/pool/plugins/com.fortify.plugin.remediation_
     <version>/Core/config

   - If the Eclipse IDE was installed without an installer:

     <eclipse_install_dir>/plugins/com.fortify.plugin.remediation_
     <version>/Core/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 you can set in the `fortify.properties` file.

Property Name	Description
com.fortify. AuthenticationKey	Specifies the directory used to store the encrypted Fortify Software Security Center authentication token. **Default:** `${com.fortify.WorkingDirectory}/config/EclipseRemediation.Plugin-`*<version>*
com.fortify. InstallationUserName	Specifies the default user name for logging in to Fortify Software Security Center for the first time. **Default:** `${user.name}`
com.fortify. remediation.PaginateIssues	If set to `true` or if no value is specified, the Fortify Remediation Plugin for Eclipse uses pagination during issue download. If set to `false`, the Fortify Remediation Plugin for Eclipse downloads all the issues at once. **Default:** `true`
com.fortify. remediation.PaginationCoun	If `com.fortify.remediation.PaginateIssues` is set to `true`, specifies the number of issues to display per subfolder.

Property Name	Description
†	**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 access to the directory. **Defaults:** • Windows—${win32.LocalAppdata}/Fortify • Non-Windows—${user.home}/.fortify

Locating Log Files

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

• On Windows:

  C:\Users*<username>*\AppData\Local\Fortify\EclipseRemediation.Plugin-*<version>*\log

• On Linux and macOS:

  <userhome>/.fortify/EclipseRemediation.Plugin-*<version>*/log

Send Documentation Feedback

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

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

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

Feedback on User Guide (Fortify Remediation Plugin for Eclipse 23.1.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!