Micro Focus Fortify Plugins for Eclipse

Software Version: 19.2.0

Installation and Usage Guide

Document Release Date: November 2019
Software Release Date: November 2019

Legal Notices

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

https://www.microfocus.com

Warranty

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

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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 October 15, 2019. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Contents

Preface 8
Contacting Micro Focus Fortify Customer Support 8
For More Information 8
About the Documentation Set 8

Change Log 9

Chapter 1: Introduction 10
Fortify Plugin for Eclipse 10
Fortify Remediation Plugin for Eclipse 10
Related Documents 11
All Products 11
Micro Focus Fortify Software Security Center 12
Micro Focus Fortify Static Code Analyzer 12

Chapter 2: Using the Eclipse Complete Plugin 13
About Installing the Eclipse Complete Plugin 13
Installing the Eclipse Complete Plugin from Eclipse 14
Installing the Eclipse Complete Plugin from an Update Site 15
Posting the Eclipse Complete Plugin to an Internal Update Site 15
Installing the Eclipse Complete Plugin from an Update Site 15
About Re-installing After Upgrading Fortify SCA and Applications from Fortify Audit Workbench 16
Managing the License 16
Uninstalling the Eclipse Complete Plugin 16
Source Code Scanning 17
Quick Scan Mode 17
Fortify Software Security Content 17
Configuring Security Content Updates 18
Updating Security Content 20
Manually Updating Security Content 21
Importing Custom Security Content 22

Analysis Settings 22
Configuring Analysis Settings 22
Configuring Advanced Analysis Options 23
Scanning in Full Scan or Quick Scan Mode 23
Specifying Additional Fortify Static Code Analyzer Options 24
About the Scan Results File Name and Directory 24
Making Changes for all Projects 24
Making Changes for Specific Projects 25
Specifying Resources to Scan 25
Viewing the Resources and Classpath to be Scanned 25
Scanning Projects 26
Scanning Individual Files and Packages 26
Running an Advanced Analysis 26
About Viewing Scan Results 30
Static Analysis Results View 31
Filter Sets 32
Specifying the Default Filter Set 33
Folders (Tabs) 33
Group By List 34
Specifying the Default Issue Grouping 34
Sorting Issues 35
Search Box 35
Project Summary View 36
Summary Tab 36
Certification Tab 36
Build Information Tab 36
Analysis Information Tab 37
Viewing Summary Graph Information 37
Analysis Trace View 41
Issue Auditing View 43
Audit Tab 43
Details Tab 44
WebInspect Agent Details Tab 45
Recommendations Tab 45
History Tab 46
Diagram Tab 46
Filters Tab 46
Warnings Tab 47

Viewing Issues in the Source Code 49
Working with Issues 49
Filtering Issues with Audit Guide 49
Grouping Issues 51
Creating a Custom Group By Option 53
Evaluating Issues 55
Performing Quick Audits 55
Performing Quick Audits for Custom Tags 56
Adding Screen Captures to Issues 56
Viewing Images 57
Creating Issues for Undetected Vulnerabilities 57
Suppressing Issues 57
Creating Attribute Summary Tables for Multiple Issues 58
Customizing the Static Analysis Results View 60
Submitting an Issue as a Bug 62
Integrating with a Bug Tracker Application 63
Configuring Proxy Settings for Bug Tracker Integration 63
Searching for Issues 64
Search Modifiers 65
Search Query Examples 71
Performing Simple Searches 72
Performing Advanced Searches 73
Eclipse Complete Plugin Reports 74
Opening Legacy Report Templates 74
Generating Legacy Reports 75
Legacy Report Templates 76
Selecting Report Sections 77
Editing Report Subsections 77
Editing Text Subsections 77
Editing Results List Subsections 79
Editing Charts Subsections 79
Saving Legacy Report Templates 79
Saving Changes to Report Templates 80
Report Template XML Files 80
Adding Report Sections 80
Adding Text Subsections 81
Adding Results List Subsections 81
Adding Charts Subsections 82

Configuring a Connection to Fortify Software Security Center 83
Logging in to Fortify Software Security Center 84
Synchronizing with Fortify Software Security Center 84
Scheduling Synchronization 85
Refreshing Permissions From Fortify Software Security Center 85
Working with Audit Projects 86
Opening an Audit Project 86
Opening an Existing Audit 86
Opening Audit Projects Without the Default Filter Set 86
Exporting an Audit Project 87
Obtaining New Results 87
Merging Audit Data 87
Performing a Collaborative Audit 88
Uploading Audit Results to Fortify Software Security Center 88
About Issue Templates 89
Configuring Custom Filter Sets and Filters 90
Creating a New Filter Set 91
Creating a Filter from the Static Analysis Results View 91
Creating a Filter from the Issue Auditing View 92
Copying a Filter from One Filter Set to Another 93
Committing Filter Sets and Folders 93
Synchronizing Filter Sets and Folders 94
Setting the Default Filter Set 94
Managing Folders 95
Creating a Folder 95
Adding a Folder to a Filter Set 96
Renaming a Folder 97
Removing a Folder 97
Configuring Custom Tags for Auditing 98
Adding a Custom Tag 99
Hiding a Custom Tag 100
Committing Custom Tags to Fortify Software Security Center 101
Synchronizing Custom Tags with Fortify Software Security Center 101
Issue Template Sharing 102
Exporting an Issue Template 102
Importing an Issue Template 102
Troubleshooting 103
Resolving the Java OutOfMemory Message 103

Resolving Scan Failures Due to Insufficient Memory 103
Saving a Project That Exceeds the Maximum Removed Issues Limit 104
Using the Debugging Option 104

Chapter 3: Using the Eclipse Remediation Plugin 106
Installing the Eclipse Remediation Plugin 106
Installing the Eclipse Remediation Plugin Locally 106
Installing the Eclipse Remediation Plugin from an Update Site 107
Posting the Eclipse Remediation Plugin to an Internal Update Site 107
Installing From an Update Site 107
Uninstalling the Eclipse Remediation Plugin from Eclipse 108
Opening a Fortify Software Security Center Application Version 108
Remediation View 109
Issues List 109
Grouping and Viewing Issues 110
Customizing the Issues List 111
Audit Tab 112
Assigning Users to Issues 112
Assigning Tags to Issues 112
Adding Comments to Issues 113
Recommendations Tab 113
Details Tab 113
History Tab 114
Locating the Source Code Associated with Issues 114
Eclipse Remediation Plugin Reports 115
Generating Reports 115
Downloading Reports From Fortify Software Security Center 115

Send Documentation Feedback 116

Preface

Contacting Micro Focus Fortify Customer Support

If you have questions or comments about using this product, contact Micro Focus Fortify Customer Support using one of the following options.

To Manage Your Support Cases, Acquire Licenses, and Manage Your Account

https://softwaresupport.softwaregrp.com

To Call Support

1.844.260.7219

For More Information

For more information about Fortify software products:
https://software.microfocus.com/solutions/application-security

About the Documentation Set

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

https://www.microfocus.com/support-and-services/documentation

Change Log

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

Software Release / Document Version	Change
19.2.0	Updated: • "Issue Auditing View" on page 43 - Tab names were changed to be consistent with Micro Focus Fortify Software Security Center
19.1.0	Updated: • "About Installing the Eclipse Complete Plugin" on page 13 - Any required third-party dependencies are automatically installed • "Running an Advanced Analysis" on page 26 - The option to enable Findbugs for the advanced scan was removed
18.20	Updated: • "Importing Custom Security Content" on page 22 - Added instructions for how to import custom external metadata

Chapter 1: Introduction

This guide provides information about how to install and use the Fortify Plugins for Eclipse.

This section contains the following topics:

Fortify Plugin for Eclipse 10
Fortify Remediation Plugin for Eclipse 10
Related Documents 11

Fortify Plugin for Eclipse

The Fortify Plugin for Eclipse (Eclipse Complete Plugin) consists of three separate plugin components:

- Audit—Enables you to open existing scan results and audit them. These results include detailed descriptions of the security vulnerabilities detected and recommended remediation strategies. The audit plugin component helps security code inspection by enabling you to easily navigate to the source code location associated with each vulnerability, and then prioritize and audit the results.
- Analysis—Enables you to initiate a Micro Focus Fortify Static Code Analyzer scan and analysis with Fortify security content, view the results, and fix the code associated with uncovered issues, all within the Eclipse IDE.
- Collaboration—Includes server-related functionality such as connecting to Micro Focus Fortify Software Security Center, uploading results to Fortify Software Security Center, and performing collaborative audits. (If you do not want this functionality, then there is no need to install the collaboration plugin.)

Note: For information about supported versions of Eclipse and Eclipse-based IDE versions, see the *Micro Focus Fortify Software System Requirements* document.

For instructions on how to install and use the Eclipse Complete Plugin, see "Using the Eclipse Complete Plugin" on page 13.

Fortify Remediation Plugin for Eclipse

The Fortify Remediation Plugin for Eclipse (Eclipse Remediation Plugin) works in conjunction with Micro Focus Fortify Static Code Analyzer to add remediation functionality to your software security analysis from the Eclipse IDE. The Eclipse Remediation Plugin is a lightweight plugin option for developers who do not need the scanning and auditing capabilities of Audit Workbench and the Eclipse Complete Plugin.

The Eclipse Remediation Plugin enables developers to quickly and easily understand the reported vulnerabilities and implement appropriate solutions.

Developers can address security issues while they write code in Eclipse. Your organization can use the Eclipse Remediation Plugin with Fortify Software Security Center to manage projects and assign specific issues to the relevant developers.

For instructions on how to install and use the Eclipse Remediation Plugin, see "Using the Eclipse Remediation Plugin" on page 106.

Related Documents

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

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

All Products

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

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

Micro Focus Fortify Software Security Center

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

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

Micro Focus Fortify Static Code Analyzer

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

Document / File Name	Description
Micro Focus Fortify Static Code Analyzer User Guide SCA_Guide_<*version*>.pdf	This document describes how to install and use Fortify Static Code Analyzer to scan code on many of the major programming platforms. It is intended for people responsible for security audits and secure coding.
Micro Focus Fortify Static Code Analyzer Custom Rules Guide SCA_Cust_Rules_Guide_<*version*>.zip	This document provides the information that you need to create custom rules for Fortify Static Code Analyzer. This guide includes examples that apply rule-writing concepts to real-world security issues. **Note:** This document is included only with the product download.

Chapter 2: Using the Eclipse Complete Plugin

This section contains the following topics:

About Installing the Eclipse Complete Plugin 13
Source Code Scanning 17
Fortify Software Security Content 17
Analysis Settings 22
Scanning Projects 26
About Viewing Scan Results 30
Working with Issues 49
Searching for Issues 64
Eclipse Complete Plugin Reports 74
Configuring a Connection to Fortify Software Security Center 83
Working with Audit Projects 86
About Issue Templates 89
Troubleshooting 103

About Installing the Eclipse Complete Plugin

Before you install the plugin in Eclipse, you must have selected the Eclipse Plugin during your Micro Focus Fortify Static Code Analyzer installation.

You have the follow options for installing the Eclipse Complete Plugin:

- "Installing the Eclipse Complete Plugin from Eclipse" on the next page
- "Installing the Eclipse Complete Plugin from an Update Site" on page 15

To update from an earlier Eclipse Complete Plugin version, you must first remove the existing version. For information about how to uninstall the plugin, see About Uninstalling the Eclipse Complete Plugin.

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

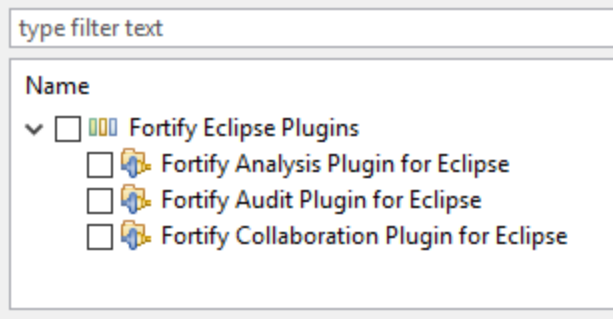
Installing the Eclipse Complete Plugin from Eclipse

To install the Eclipse Complete Plugin locally:

1. Start Eclipse.
2. Select **Help > Install New Software**.
3. Click **Add**.

   The Add Repository dialog box opens.
4. To create a local update site on your file system (as opposed to one on the Internet):
   a. (Optional) In the **Name** box, type a name for the local update site.
   b. Click **Local**, and then browse to and select the *<sca_install_dir>*/plugins/eclipse directory.
   c. Click **Add**.

   In the Install window, the **Work with** list displays the name and location of your local update site and the **Fortify Eclipse Plugins** node is listed as available software.
5. Expand the **Fortify Eclipse Plugins** node and select the check boxes for the features you want to install.



Note: Any required third-party dependencies are automatically installed if they do not already exist on your system.

6. If you have Eclipse Java Development Tools (JDT) installed, you can clear the **Contact all update sites during install to find required software** check box to reduce the installation time.

Note: Only the Fortify Analysis Plugin for Eclipse feature requires JDT.

7. Click **Next**.

   The **Install Details** step lists the plugins you selected.
8. To display version and copyright information for a plugin in the **Details** section, click the feature name.
9. Click **Next**.
10. On the **Review Licenses** step, review and accept the terms of the Micro Focus license agreement.
11. Click **Finish**.
12. To complete the installation and restart Eclipse, click **Restart Now** when prompted.

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

Installing the Eclipse Complete Plugin from an Update Site

An alternative to requiring every developer to install the Eclipse Complete Plugin locally is to post the plugin to an internal update site that can serve as a single distribution point. The only requirement is that you have an internal web server.

Posting the Eclipse Complete Plugin to an Internal Update Site

To post the plugin for other users to access:

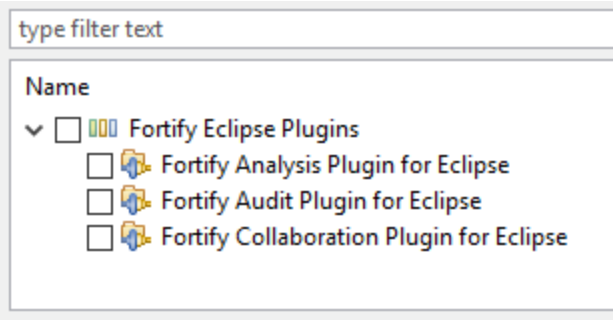
1. Copy the contents of *<sca_install_dir>*/plugins/eclipse directory on to your web server.
2. Provide the URL for the update site to the appropriate users.

Installing the Eclipse Complete Plugin from an Update Site

To install the Eclipse Complete Plugin after it has been posted to an update site:

1. Obtain the URL of the plugin update site for your organization.
2. Select **Help > Install New Software**.
3. Click **Add**.
4. In the **Name** box, type a name for the update site.
5. In the **Location** box, type the URL of the update site.
6. Click **OK**.

   In the Install window, the **Work with** list displays the update site you specified and the **Fortify Eclipse Plugins** node is listed as available software.
7. Expand the **Fortify Eclipse Plugins** node, select the **Fortify Eclipse Plugins** check box, and then select the check box or check boxes for the plugins you want to install.



Note: Any required third-party dependencies are automatically installed if they do not already exist on your system.

8. Click **Next**.

   The **Install Details** step lists the plugins you selected.

9. To display version and copyright information about the plugin in the **Details** box, click the plugin name.
10. Click **Next**.
11. On the **Review Licenses** step, review and accept the terms of the Micro Focus license agreement.
12. Click **Finish**.
13. Click **OK**.
14. To complete the installation, click **Yes** to restart Eclipse when prompted.

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

About Re-installing After Upgrading Fortify SCA and Applications from Fortify Audit Workbench

If you have upgraded Fortify SCA and Applications from Audit Workbench, you must uninstall, and then reinstall the Eclipse Complete Plugin. For information about how you can upgrade the Fortify SCA and Applications from Fortify Audit Workbench, see the *Micro Focus Fortify Audit Workbench User Guide*.

Managing the License

The Fortify license enables you to scan your code with the Eclipse Complete Plugin. For information about how to obtain a Fortify license file, see the *Micro Focus Fortify Software System Requirements* document.

To update your license file:

1. Select **Fortify > Manage License**.
2. Click **Browse** and locate the license file on your computer, and then click **OK**.

Uninstalling the Eclipse Complete Plugin

You can uninstall the Eclipse Complete Plugin from either Eclipse or from the command line. See the Eclipse instructions for how to remove installed software from Eclipse.

An uninstall script is in the `<sca_install_dir>/plugins/eclipse` directory.

To uninstall all the Fortify Eclipse plugins from the command line:

1. Close Eclipse if it is open.
2. Run the uninstall script for your operating system:
   - On Windows, run `uninstall_fortify_plugins.cmd`.
   - On Linux or macOS, run `uninstall_fortify_plugins.sh`.
3. Type the location of the folder that contains the Eclipse executable.

Source Code Scanning

If you installed the analysis plugin component, you can initiate a scan and analysis of your Java source code from Eclipse. Micro Focus Fortify Static Code Analyzer scans are invoked from Eclipse Complete Plugin with the server Java Virtual Machine.

The scan and analysis processes clean up old source code analysis files, rebuild the solution if necessary, translate source code files, perform the security analysis, and then display the results in Eclipse.

Best Practices

- Fortify recommends that you periodically update the security content. For instructions, see "Updating Security Content" on page 20.
- To get the best results from your scans, before you scan your project source code, make sure that you can compile the project with no errors.

Quick Scan Mode

With quick scan mode, you can quickly scan projects for major issues. For example, a quick scan of the WebGoat sample application uncovers approximately 75% fewer issues than a full scan of the same application.

In quick scan mode, Micro Focus Fortify Static Code Analyzer searches for high-confidence, high-severity issues. Quick scans are a great way to get many applications through an assessment so that you can quickly find issues and begin remediation. Although the scan is faster than a full scan, it does not provide as robust a result set. Critical and other issues that a quick scan cannot detect may exist in your application. Fortify recommends that you run full scans whenever possible.

Note: By default, Micro Focus Fortify Software Security Center ignores uploaded scans performed in quick scan mode. However, you can configure your Fortify Software Security Center application version so that uploaded audit projects scanned in quick scan mode are processed. For more information, see analysis results processing rules in the *Micro Focus Fortify Software Security Center User Guide*.

To configure your scan to run in full scan or quick scan mode, see "Scanning in Full Scan or Quick Scan Mode" on page 23.

Fortify Software Security Content

The Eclipse Complete Plugin uses a knowledge base of rules to enforce secure coding standards applicable to the codebase for static analysis. Fortify software security content consists of Fortify Secure Coding Rulepacks and external metadata:

- Fortify Secure Coding Rulepacks describe general secure coding idioms for popular languages and public APIs

- External metadata provides mappings from the Fortify vulnerability categories to alternative categories (such as CWE, OWASP Top 10, and PCI)

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

Fortify recommends that you periodically update the security content.

For more information, see:

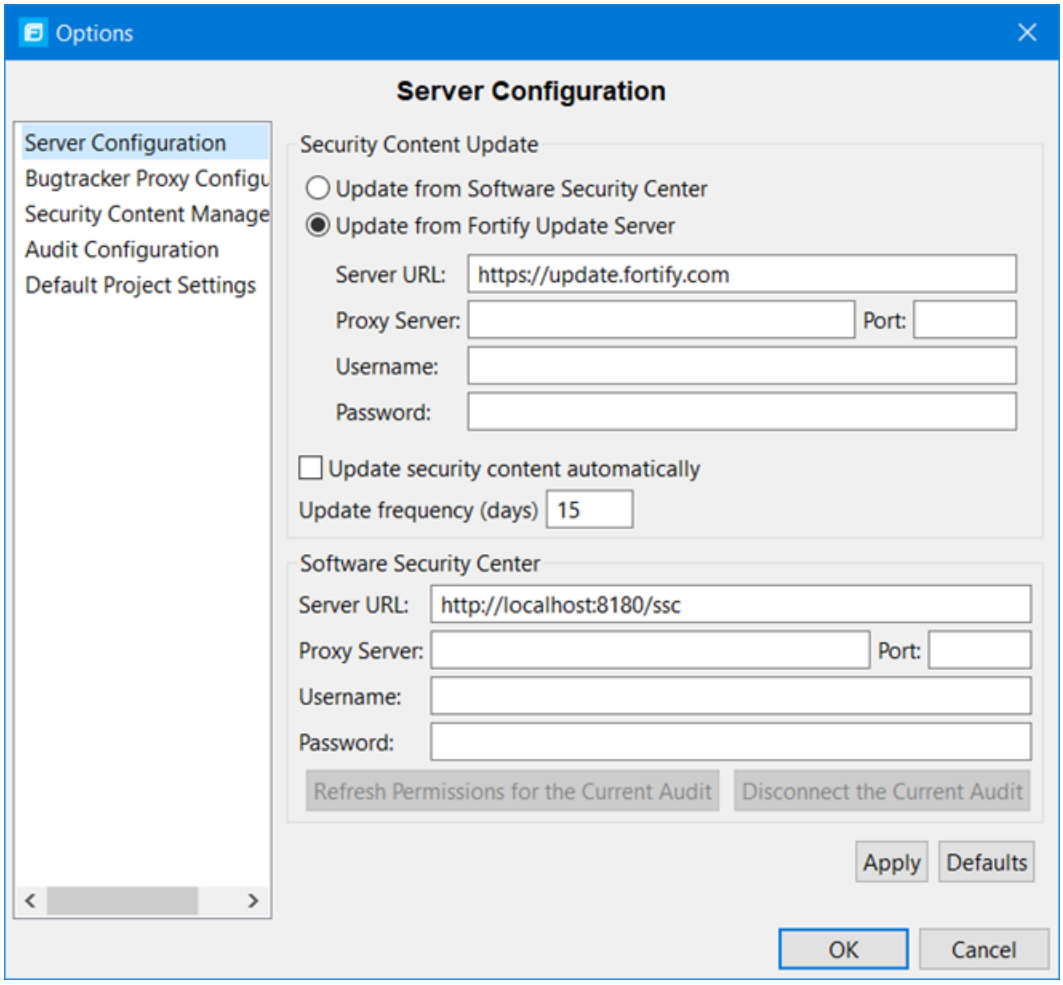
- "Configuring Security Content Updates" below
- "Updating Security Content" on page 20
- "Manually Updating Security Content" on page 21
- "Importing Custom Security Content" on page 22

Configuring Security Content Updates

If the analysis plugin component is installed, you can specify the server information to use to update security content. To update security content manually (without an Internet connection or Micro Focus Fortify Software Security Center), see "Manually Updating Security Content" on page 21.

To configure security content updates:

1. Select **Fortify > Options**.
2. In the left panel, select **Server Configuration**.



3. To update security content from your Fortify Software Security Center server:
   a. Under **Security Content Update**, select the **Update from Software Security Center** check box.

      Note: If this check box is unavailable, then click **Security Content Management** in the left panel and if prompted to locate the Fortify Static Code Analyzer executable location, click **OK** and specify its location.

   b. Under **Software Security Center**, specify the Fortify Software Security Center server URL and if necessary, the proxy server, port number, and optionally credentials for proxy authentication.
4. To specify an update server from which to update security content, under **Security Content Update**, do the following:
   a. In the **Server URL** box, type the URL for the update server.
   b. If required, specify the proxy server, port number, and optionally credentials for proxy authentication.

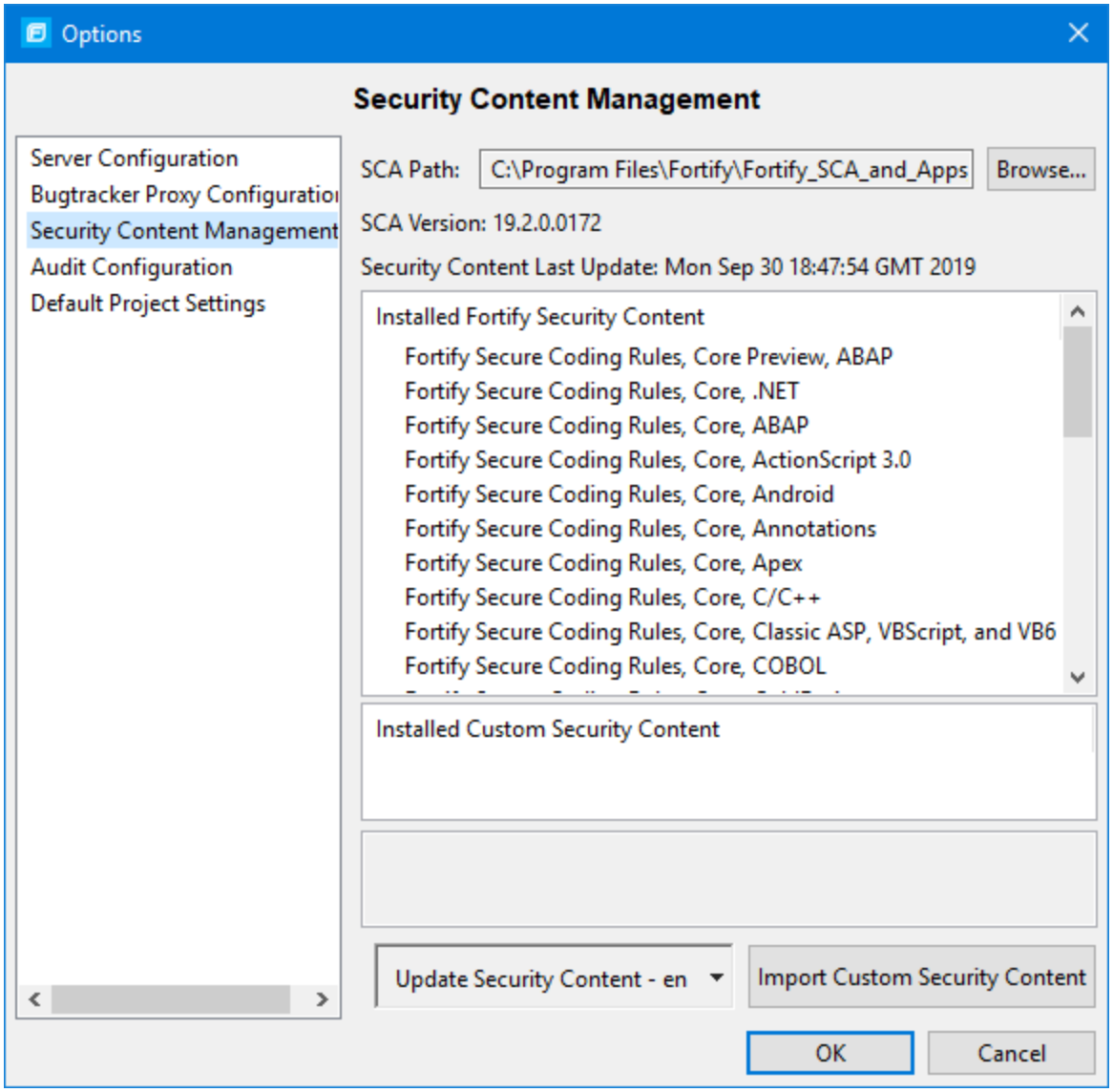
5. To update security content automatically and with a specific frequency:
   a. Select the **Perform security content update automatically** check box.
   b. In the **Update frequency (days)** box, specify how often (type the number of days) you want the security content automatically updated.
6. Click **Apply**, and then click **OK**.

Updating Security Content

Fortify provides security content in English, Spanish, Brazilian Portuguese, Japanese, Korean, Simplified Chinese, or Traditional Chinese. Issue descriptions and recommendations are available in the selected language and the Fortify categories are in English.

To update your security content:

1. Select **Fortify > Options**.
2. In the left panel, select **Security Content Management**.



Note: Scroll to the bottom of the **Installed Fortify Security Content** list to see the external mappings.

Any custom rules and custom external mappings appear in the **Installed Custom Security Content** list.

3. In the **Update Security Content** list, select the security content in the language you want.

   The Security Content Update window displays the results of the security content update.
4. Click **OK** to close the Security Content Update window.

Manually Updating Security Content

You can manually update security content from a local ZIP file with the fortifyupdate utility.

To manually update your security content:

1. Open a command prompt window, and then navigate to the *<sca_install_dir>*/bin directory.
2. At the prompt, type the following:

```
fortifyupdate -import <file>.zip
```

For more information about the fortifyupdate utility, see the *Micro Focus Fortify Static Code Analyzer User Guide*.

Importing Custom Security Content

You can import custom security content to use in your scans.

Note: To import custom external metadata, place your external metadata file in the *<sca_install_dir>*/Core/config/CustomExternalMetadata directory.

To import custom rules, do the following:

1. Select **Fortify > Options**.
2. In the left panel, select **Security Content Management**.
3. Click **Import Custom Security Content**.
4. Select the custom rules file you want to import, and then click **Open**.

Note: Custom security content is only supported with static analysis.

Analysis Settings

You can customize your scan and analysis settings to suit your requirements. You also have the option to run scans in quick scan mode. The following sections provide instructions about how to configure your scans and how to use quick scan mode.

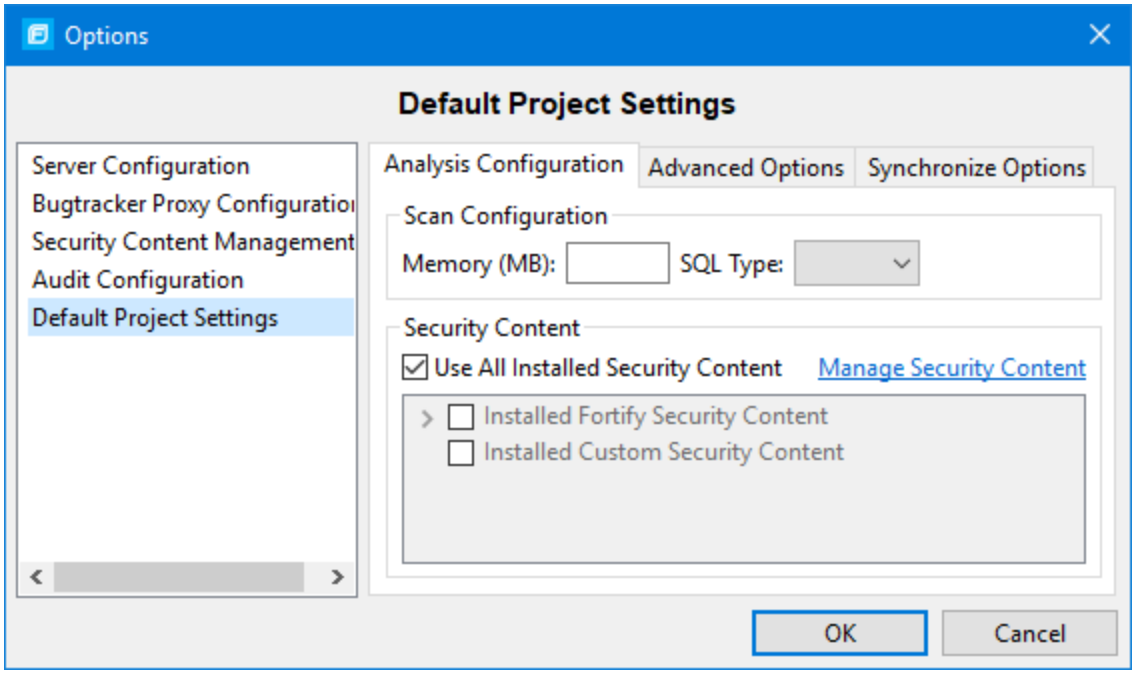
Configuring Analysis Settings

The source code analysis settings are available only if the analysis plugin is installed. The source code analysis settings enable you to configure security content and amount of memory Micro Focus Fortify Static Code Analyzer uses during the scan.

To configure the analysis settings:

1. Select **Fortify > Options**.
2. Select **Default Project Settings**.

The **Analysis Configuration** tab opens.



3. To specify the amount of memory to use for the scan, type an integer in the **Memory (MB)** box.

   Note: Do not allocate more than two thirds of the available physical memory.

4. By default, Fortify Static Code Analyzer treats SQL files as though they use the T-SQL procedural language on Windows systems and PL/SQL on other platforms. To specify the SQL type, click the **SQL Type** menu, and then select **TSQL** or **PLSQL**.
5. To use specific security content to scan the project (instead of all security content), under **Security Content**, clear the **Use All Installed Security Content** check box, and then select the check boxes for the installed Fortify and custom security content to use.
6. To update or import custom security content, click **Manage Security Content**.
7. Click **OK**.

Configuring Advanced Analysis Options

This section describes how to configure advanced analysis options. These options are available only if the analysis plugin is installed.

Scanning in Full Scan or Quick Scan Mode

To enable or disable quick scan mode:

1. Select **Fortify > Options**.
2. In the left panel, select **Default Project Settings**.
3. In the right panel, select the **Advanced Options** tab.

4. Under **Advanced Analysis Options**, select or clear the **Enable quick scan mode** check box.
5. Click **OK**.

Specifying Additional Fortify Static Code Analyzer Options

To specify additional Micro Focus Fortify Static Code Analyzer options:

1. Select **Fortify > Options**.
2. Select **Default Project Settings**.
3. Click the **Advanced Options** tab.
4. Select **Use Additional SCA Arguments** and then type command line options for either the translation or scan phase.

   For example, if you include the `-verbose` command-line option, detailed status messages are sent to the console during the analysis.

   For information about the available command-line options and syntax format, see the *Micro Focus Fortify Static Code Analyzer User Guide*.
5. Click **OK**.

About the Scan Results File Name and Directory

By default, after you scan a project, the Eclipse Complete Plugin assigns the results file (FPR file) a name in the format `<project_name>Scan.fpr` and places it in a new project folder in your Eclipse working directory. You can, if you prefer, store your project scan results file under a different name and directory.

To change the default directory and FPR file name for all projects, use the Options dialog box. To change the default directory and FPR file name for a specific project, use the Eclipse Properties window.

Making Changes for all Projects

To specify a default FPR file name and directory for all projects:

1. Select **Fortify > Options**.
2. In the left panel, select **Default Project Settings**.
3. In the right panel, select the **Advanced Options** tab.
4. Select the **Use Additional SCA Arguments** check box.
5. Do one of the following:
   - In the **Output results to** box, type the absolute path for FPR files.
   - To specify a name and a static workspace folder for FPR files, click **Workspace**, and then, in the Folder Selection window, navigate to and select a workspace relative directory.
   - To specify a name and a static folder that is *not* part of your workspace, click **File System**, and then select a directory for FPR files.

- To specify a name and a dynamic path that changes based on the project you are analyzing, click **Variables**, and then, in the Select Variable window, select core Eclipse variables to specify the relative path for FPR files.

Making Changes for Specific Projects

To specify a default FPR file name and directory for a specific project:

1. From the Java perspective in Eclipse, right-click a project name, and then select **Properties** from the shortcut menu.

   The Properties for <*project_name*> window opens.
2. In the left panel, select **Fortify Project Properties**.
3. In the right panel, select the **Enable Project Specific Settings** check box.
4. In the right panel, click the **Advanced Options** tab.
5. Select the **Use Additional SCA Arguments** check box.
6. Do one of the following:
   - In the **Output results to** box, type the absolute path for project FPR files.
   - To specify a name and a static workspace folder for project results, click **Workspace**, and then, in the Folder Selection dialog box, navigate to and select a workspace relative directory.
   - To specify a name and a static folder that is *not* part of your workspace, click **File System**, and then select a directory for FPR files.
   - To specify a name and a dynamic path that changes based on the project you are analyzing, click **Variables**, and then, in the Select Variable dialog box, select core Eclipse variables to specify the relative path for the FPR files.

Specifying Resources to Scan

The Eclipse Complete Plugin automatically includes all source files from dependent projects in scans of selected projects. For JAR files included in the project you select to scan, if the source exists in the workspace for a given JAR, the Eclipse Complete Plugin includes the source in the scan.

Viewing the Resources and Classpath to be Scanned

To see the project resources and classpath to be scanned for a project:

1. From the Java view in Eclipse, do one of the following:
   - Right-click a project name, and then select **Advanced Analysis** from the shortcut menu.
   - Select a project name, and then select **Fortify > Advanced Analysis**.

   The Advanced Static Analysis wizard opens.
2. Expand the directory tree.

The Advanced Static Analysis displays the project resources and classpath to be scanned. If you have "Scan resources in dependent projects" enabled, you can see any dependent projects in the **Workspace**

Source Dependencies root. If you have a source code folder set up for any of the referenced libraries and it is not in your workspace, it is listed in the **External Source Dependencies** folder. All library JAR files configured for your project that are not under the root of your project are shown in the **External Classpath** folder.

Scanning Projects

The Eclipse Complete Plugin automatically includes all source files from dependent projects in scans. Although you can scan individual packages and files (see "Scanning Individual Files and Packages" below), the results are more accurate if you scan an entire project at once.

Note: You can scan multiple projects at the same time with the advanced analysis (see "Running an Advanced Analysis" below).

To scan a project:

1. Open the project in the Java perspective.
2. In the **Package Explorer** or **Project Explorer** view, select the project.
3. Select **Fortify > Analyze Project**.

After the scan finishes, the results are loaded into and displayed in the Fortify Audit perspective.

Scanning Individual Files and Packages

You can also scan individual files and packages.

Note: Fortify does not recommend this method, because analysis results are more accurate when an entire project is scanned at once.

To scan individual files or packages:

1. From Eclipse, open the project in the Java perspective.
2. In the **Package Explorer** view, right-click the file or package to scan, and then select **Analyze Project Component** from the shortcut menu.

Running an Advanced Analysis

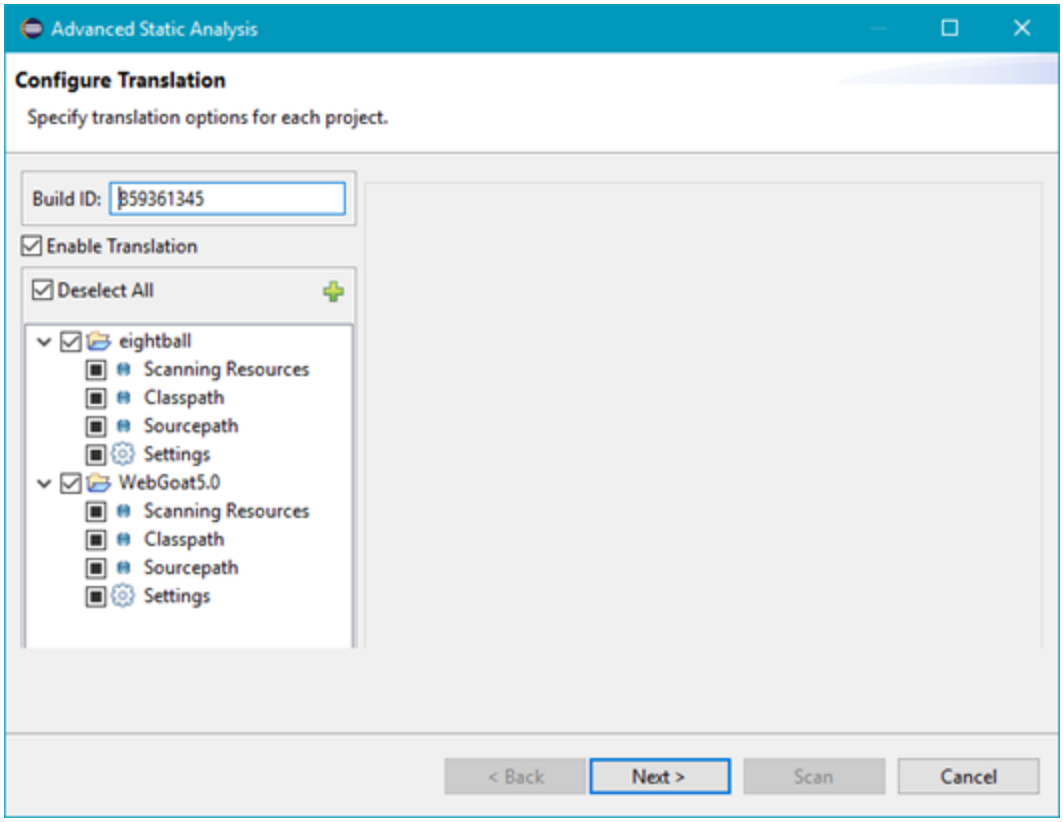
Use the advanced analysis for Eclipse projects that have source code in multiple directories, special translation or build conditions, or that have files that you want to exclude from the project. With advanced analysis, you can scan Java projects, JavaScript projects, PHP projects, C/C++ projects, and all other types of projects that you can create in Eclipse.

Note: The Eclipse Complete Plugin filters out unsupported files within the selected source code directories.

To perform an advanced analysis:

1. Select one or more Eclipse projects.
2. Select **Fortify > Advanced Analysis**.

   The Advanced Static Analysis wizard opens.



   The selected Eclipse projects to be scanned are listed in the left panel.
3. In the Build ID box, type the build ID.

   If you selected only one project for the advanced analysis, the first root directory is the default build ID. Otherwise, the wizard creates unique number for the Build ID, which you can change.
4. To disable translation, clear the **Enable Translation** check box.

   For example, if the security content has changed but the source code has not, you might want to disable the translate phase so that the project is scanned without retranslating.

   Note: Selection of the **Enable Translation** option directs the wizard to perform the Micro Focus Fortify Static Code Analyzer clean phase for the build ID in addition to the source code translation. During the clean phase, Fortify Static Code Analyzer removes temporary files from previous translation of the project. If translation is disabled, the clean phase is also not performed.
5. To add additional Eclipse projects for analysis, click **Add Project** above the Eclipse projects list on the left.

The wizard automatically includes all supported files in the translation as determined by the project type. For Java projects, the wizard uses Eclipse logic to resolve source paths. For non-Java projects, the wizard includes all files under the project root.

- **Scanning Resources**—Source files for translation.

  Make sure only the files or directories that you want to translate are selected. To add additional files for translation, click **Add Files** .

- **Classpath**—(Java projects only) The classpath to use for the Java source code. Include all JAR dependencies normally used to build the project.

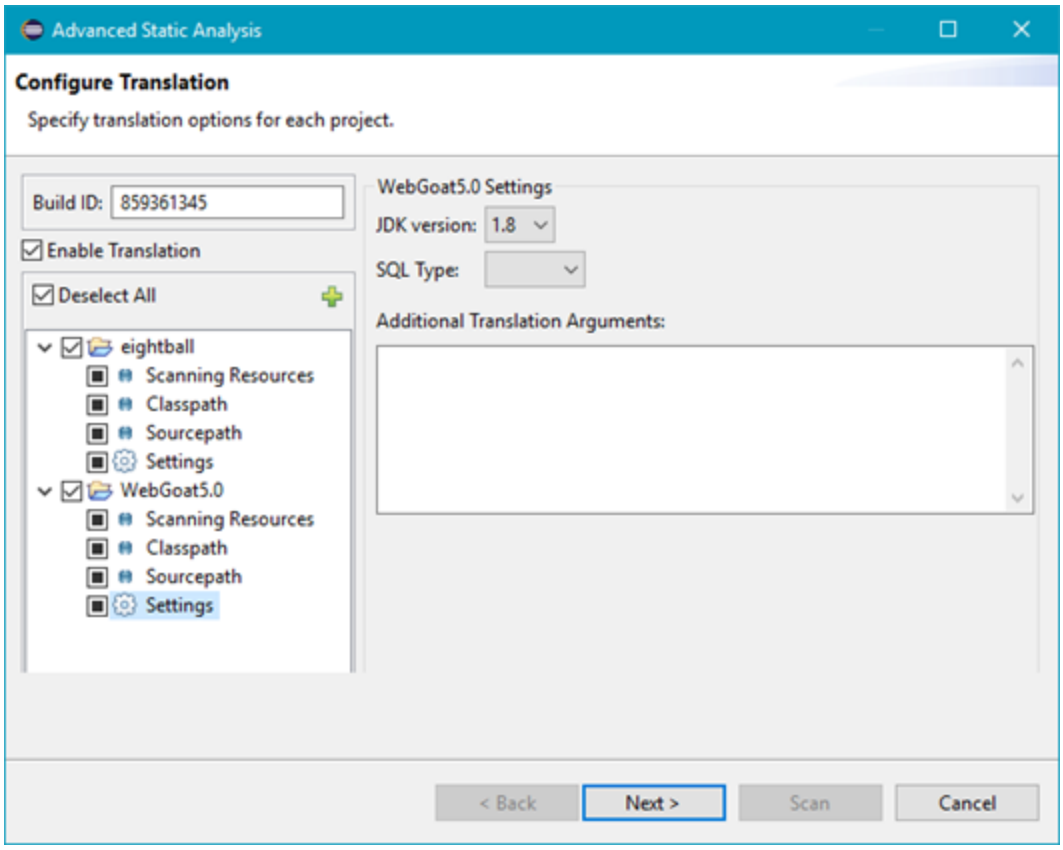
  Make sure to select only the files or directories that you want to translate. To add additional files for translation, click **Add Folders** . To add JAR files, click **Add JAR** .

- **Sourcepath**—(Java projects only) Folders that contain source code of dependent projects.

  To add additional files for translation, click **Add Folders** .

6. Click **Settings** for each Eclipse project to specify additional translation options.

Note: The translation setting options available depend on the Eclipse project type. The following image shows the options for a Java project.



a. From the **JDK version** list, select the Java version of the code in the project.

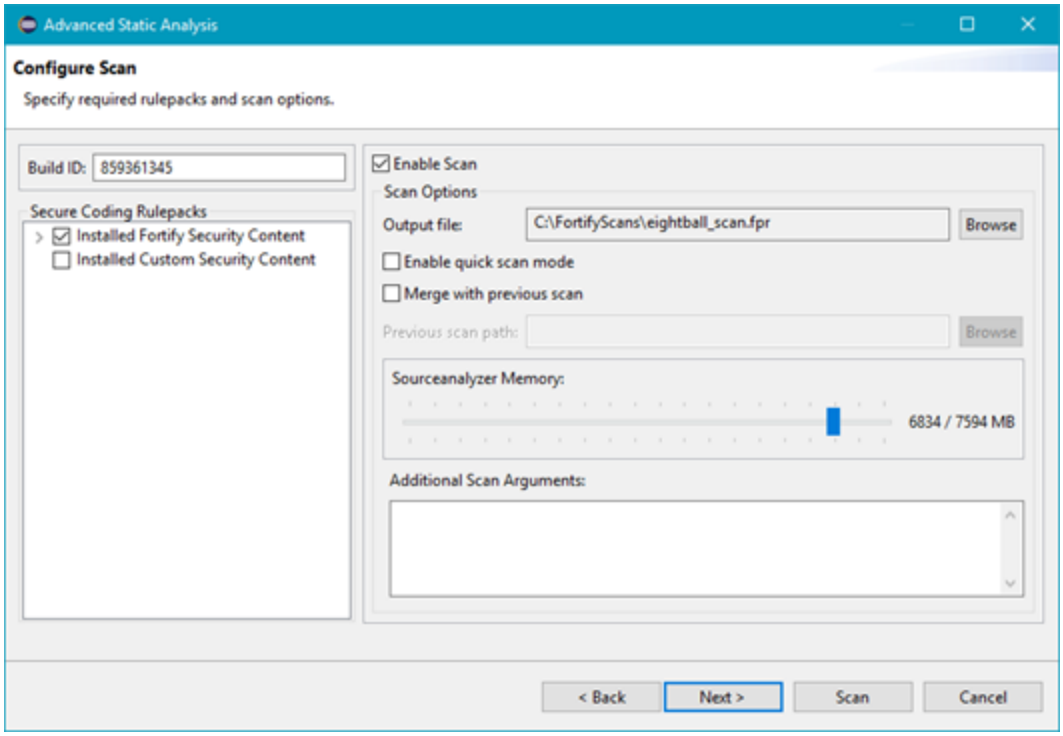
b. By default, Micro Focus Fortify Software Security Center treats SQL files as though they use the T-SQL procedural language on Windows systems and PL/SQL on other platforms. To

specify the SQL type, click the **SQL Type** menu, and then select **TSQL** or **PLSQL**.

c. Specify any additional translation options in the **Additional Translation Arguments** box.

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

7. Click **Next** to configure the scan options.



a. (Optional) To skip the scan phase, clear the **Enable Scan** check box.

For example, if you want to offload the scan phase to a different machine, you would skip the scan phase, use the command line to create a mobile build session (MBS) file, and import the MBS to the scan machine. See the *Micro Focus Fortify Static Code Analyzer User Guide* for instructions on how use mobile build sessions.

b. To specify a different output file path than the default, in the **Output file** box, type the path and file name for the FPR file that Fortify Static Code Analyzer is to generate.

c. To perform a quick scan, select the **Enable Quick Scan Mode** check box.

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

d. To merge these results with a previous scan, select the **Merge with previous scan** check box, and then click **Browse** to navigate to and select the previous FPR file.

e. (Optional) To specify the amount of memory Fortify Static Code Analyzer uses for scanning, adjust the slider to the amount of memory as needed.

f. (Optional) Specify any additional scan options in the **Additional Scan Arguments** box.

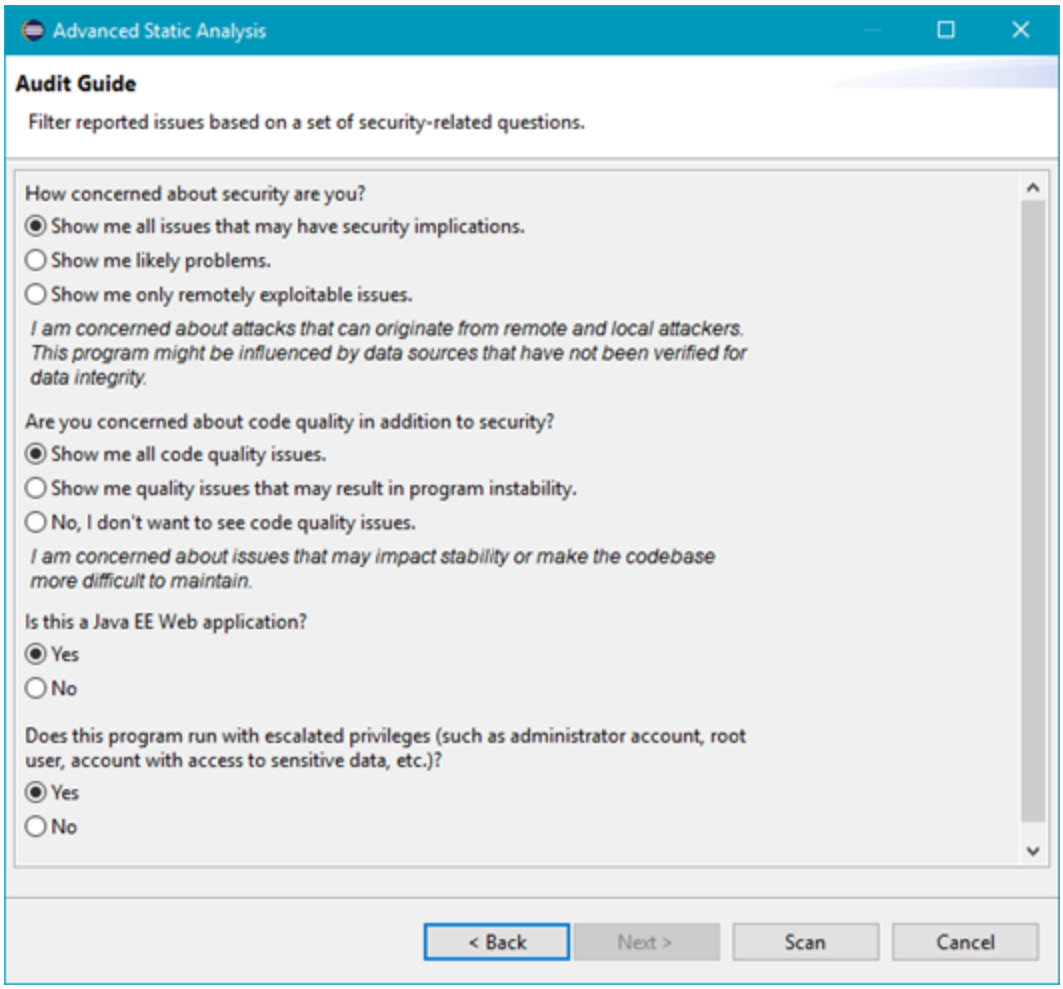
For information about the available command-line scan options, see the *Micro Focus Fortify Static Code Analyzer User Guide*.

8. (Optional) To scan the code with a custom selection of Rulepacks, do the following:

a. In the **Secure Coding Rulepacks** list in the left panel, expand the **Installed Fortify Security Content** node and display the installed Rulepacks.
b. In the **Installed Fortify Security Content** list, clear the check boxes that correspond to any Rulepacks you want to disable for the scan.

Note: For instructions on how to add custom security content, see "Importing Custom Security Content" on page 22.

9. Click **Next** to proceed to the Audit guide page or to skip the Audit Guide options, click **Scan**.



10. Select your scan settings, and then click **Scan**.

The scan starts and progress information is displayed throughout the process. If Fortify Static Code Analyzer encounters any problems scanning the source code, a warning is displayed.

After the scan is completed, the analysis results are displayed in the Fortify Audit perspective.

About Viewing Scan Results

The Fortify Audit perspective displays four audit-focused views.

After the scan is completed (or, after you open an existing audit project), summary results are displayed in the **Static Analysis Results** view and in the **Project Summary** view of the Fortify Audit perspective. The **Analysis Trace** and **Issue Auditing** views are open, but do not contain any information until you select an issue from the **Static Analysis Results** view.

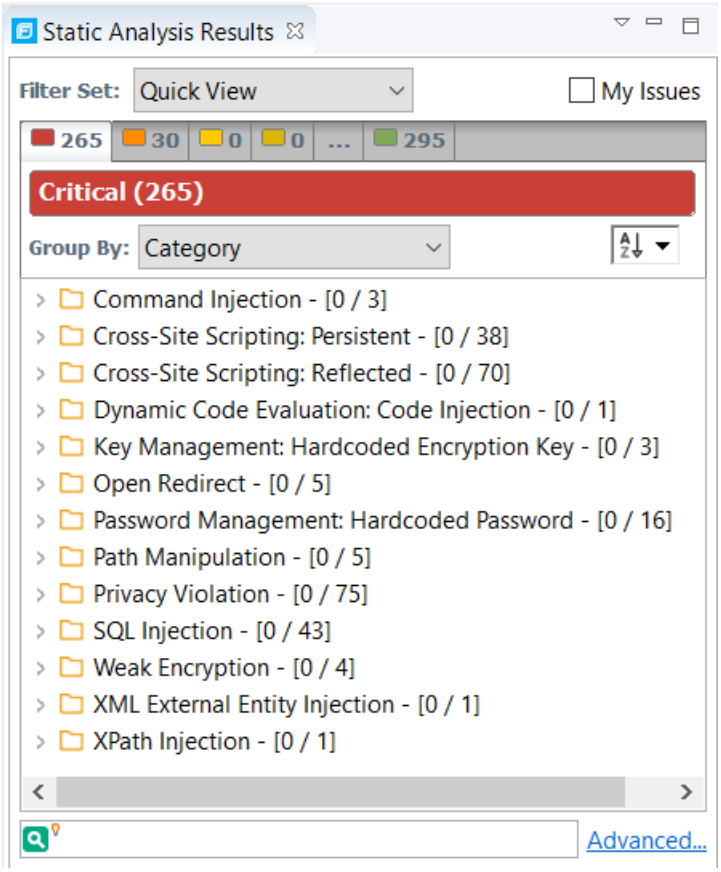
View	More Information
Static Analysis Results (top left)	"Static Analysis Results View" below
Project Summary (top center)	"Project Summary View" on page 36
Analysis Trace (bottom left)	"Analysis Trace View" on page 41
Issue Auditing (bottom center)	"Issue Auditing View" on page 43

You can also open audit-related views in other perspectives, such as the Java perspective or the C/C++ perspective, and rearrange the views. You might decide to use the audit views only, and stay within a customized development perspective.

Static Analysis Results View

The **Static Analysis Results** view provides a way to group and select the issues to audit. The view contains the **Filter Set** list, folders (tabs), the **Group By** list, the **My Issues** check box, and a search box.

Note: In this view, you can right-click an issue and select **Issue Attributes** to see all the attributes associated with the issue such as Analysis tag, analyzer that detected the issue, severity, and more.



Filter Sets

The selected filter set controls which issues are listed in the **Static Analysis Results** view. The filter set determines the number and types of containers (folders) that are shown and how and where to display issues. The default filter sets sort the issues by severity into the **Critical**, **High**, **Medium**, **Low**, and **All** folders.

Because filter sets are saved to audit project files, each audit project can have unique filter sets.

The plugin provides the following filter sets for new projects:

- **Quick View**: This is the default initial filter set for new projects. The Quick View filter set provides a view only of 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). The Quick View filter set provides a useful first look at results that enables you to quickly address the most pressing issues.
- **Security Auditor View**: This is the default filter set for projects scanned in earlier product versions. This view shows all security issues detected. The Security Auditor View filter contains no visibility filters, so all issues are shown.

For instructions on how to create custom filter sets, see "Configuring Custom Filter Sets and Filters" on page 90.

If you open an FPR file that contains no custom `filtertemplate.xml` file or if you open an FVDL file or a `webinspect.xml` file, the audit project opens with the Quick View filter set selected.

Specifying the Default Filter Set

You can change the initial filter set to use for new or opened projects. You can also disable the default filter set so that the filter set last enabled in the issue template is used to display scan results for new projects.

To select the filter set for new or opened projects:

1. Select **Fortify > Options**.
2. In the left panel, select **Audit Configuration**, and then click the **Configuration** tab on the right.
3. Under **Audit Project Load Mode**, leave the **Default Filter Set** check box selected.

   If you clear the check box, the default filter is loaded. For newly-opened projects, the default filter for FPRs that have no embedded template or the default filter from the embedded template is the Security Auditor View filter set.
4. From the list to the right of the **Default Filter Set** check box, select the filter set to use to display scan results for new projects.
5. Click **OK**.

Folders (Tabs)

The color-coded **Critical**, **High**, **Medium**, **Low**, and **All** tabs on the **Static Analysis Results** view are called folders. You can customize the folders and their settings. The number of folders, names, colors, and the issue list can vary between filter sets and projects.

Note: In the Eclipse Complete Plugin, the term folder *does not* refer to the folder icons in the issues list.

The filter set you select from the **Filter Set** list determines which folders are visible in the Static Analysis Results view. The following folders are visible while the Security Auditor View filter set is selected:

- The **Critical** folder contains issues that have a high impact and a high likelihood of occurring. Issues at this risk level are easy to discover and to exploit, and represent the highest security risk to a program. Remediate critical issues immediately.

  Example: `SQL Injection`
- The **High** folder contains issues that have a high impact and a low likelihood of occurring. High-priority issues are often difficult to discover and exploit, but can result in much asset damage. They represent a significant security risk to a program. Remediate these issues with the next patch release.

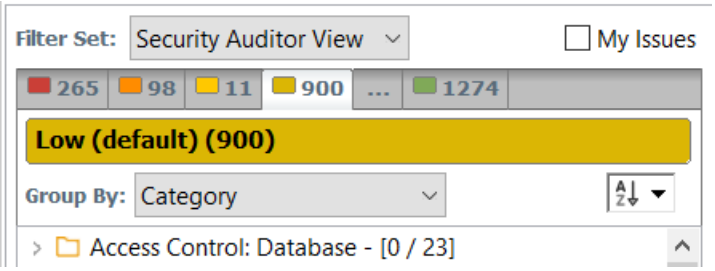
  Example: `Password Management: Hardcoded Password`
- The **Medium** folder contains issues that a have low impact and a high likelihood of exploitation. Medium-priority issues are easy to discover and exploit, but often result in little asset damage. These issues represent a moderate security risk to a program. Remediate these issues as time permits.

  Example: `ASP.NET Misconfiguration: Missing Error Handling`

- The **Low** folder contains issues that have a low impact and a low likelihood of exploitation. Remediate these issues as time permits. Low-priority issues are potentially difficult to discover and to exploit and typically result in little asset damage. These issues represent a minor security risk to the program.

  Example: `Poor Error Handling: Empty Catch Block`
- The **All** folder contains the issues from all the other folders.

An issue is listed in a folder if the folder filter conditions match the issue attributes. Each filter set has a default folder, indicated by **(default)** next to the folder name. If an issue does not match any of the folder filters, the issue is listed in the default folder.



You can create your own folders as you need them. For example, you might group all hot issues for a project into a **Hot** folder and group all warning issues for the same project into a **Warning** folder. For instructions on how to create your own folders, see "Creating a Folder" on page 95.

Each folder contains a list of all the issues with attributes that match the folder filter conditions. One folder in each filter set is the default folder, indicated by **(default)** in the folder name.

Note: To show or hide suppressed, hidden, and removed issues, set the user interface preferences from the Options dialog box (see "Customizing the Static Analysis Results View" on page 60).

Group By List

The **Group By** list options sort the issues into sub folders. The option you select is applied to all visible folders. To list all issues in the folder without any grouping, select **<none>**.

To customize the existing groups, you can specify which attributes to sort by, add or remove the attributes to create sub-groupings, and add your own grouping options.

The **Group By** settings apply to the application instance. You can apply the **Group By** option to any project opened with that instance of the application.

For more information, see "Grouping Issues" on page 51.

Specifying the Default Issue Grouping

You can change the initial Group By setting to use for new or opened projects.

To select the default Group By setting:

1. Select **Fortify > Options**.
2. In the left panel, select **Audit Configuration**, and then click the **Configuration** tab on the right.
3. Under **Audit Project Load Mode**, select the **Default Issue Grouping** check box.

If you clear the check box, the default Group By setting is set to Category.

4. From the list to the right of the **Default Issue Grouping** check box, select the grouping you want to use to sort issues.
5. Click **OK**.

Sorting Issues

There are several different ways to sort the issues in the Static Analysis Results View. Select a sort option from the **Sort** list. The following table describes the sort options.

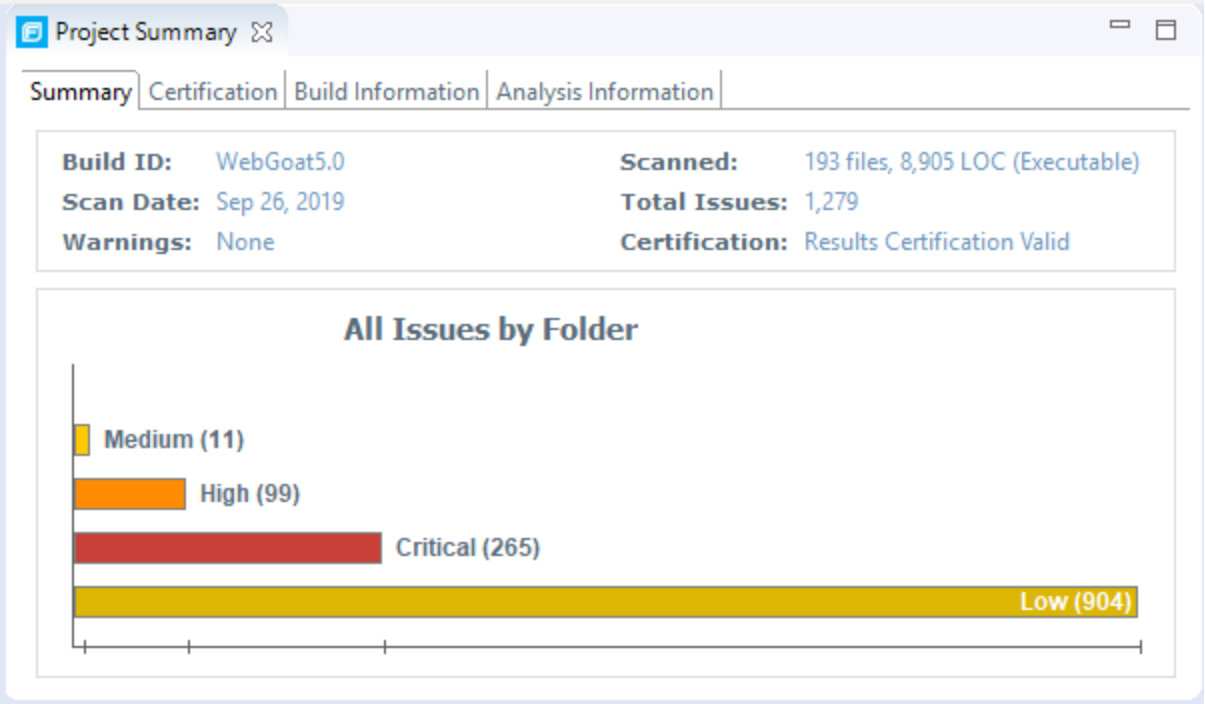
Sort Method	Icons	Description
Alphabetical		Sorts the groups and the issues within the groups in alphabetical order.
		Sorts the groups and the issues within the groups in reverse-alphabetical order
Group size		Sorts the groups by the number of contained issues from largest to smallest
		Sorts the groups by the number of contained issues from smallest to largest.
Last modified date		Sorts the groups and issues in groups by the date last modified by Micro Focus Fortify Static Code Analyzer or the audit/comment date from newest to oldest
		Sorts the groups and issues in groups by the date last modified by Fortify Static Code Analyzer or the audit/comment date from oldest to newest

Search Box

The search box enables you to limit the issues displayed in the folder and to search for specific issues. For detailed information about how to use the search box, see "Searching for Issues" on page 64.

Project Summary View

The **Project Summary** view provides detailed information about the scan.



To open this view, select **Fortify > Show Project Summary**.

Summary Tab

The **Summary** tab shows high-level information about the project. For more information, see "Viewing Summary Graph Information" on the next page.

Certification Tab

The **Certification** tab displays the result certification status and indicates whether the code analysis for a scan was complete. Results certification is a check to ensure that the analysis results have not been altered after Micro Focus Fortify Static Code Analyzer produced them. Results certification shows specific information about the scanned code, including:

- FPR certification
- Certification details such as the results and rules signatures

Build Information Tab

The **Build Information** tab displays the following information:

- Build details such as the build ID, number of files scanned, source last-modified date, and the date of the scan, which might be different than the date the files were translated

- Executable lines of code (Executable LOC) scanned - Ignore this metric. It is no longer used.
- Total lines of code (Total LOC) scanned

  This metric provides the approximate number of lines that contain code constructs (comments are excluded). The process to determine the LOC varies for the different supported languages.
- List of files scanned with file sizes and timestamps
- Libraries referenced for the scan
- Java classpath used for the translation

Analysis Information Tab

The **Analysis Information** tab shows the Fortify Static Code Analyzer version that performed the scan, details about the computer on which the scan was run, the user who started the scan, scan date, and the time required to scan the code.

The **Analysis Information** tab includes the following subtabs:

- **Security Content**—Lists information about the Rulepacks used to scan the source code
- **Properties**—Displays the Fortify Static Code Analyzer properties files settings
- **Commandline Arguments**—Displays the command-line options used to analyze the project

Viewing Summary Graph Information

The summary graph displayed in the **Project Summary** view provides multiple perspectives on the sets of issues, grouped by priority (Critical, High, Medium, and Low) uncovered in a scan. You can drill down in the graph to see detailed information about each issue set, and create various bar charts for issues based on a selected issue attribute.

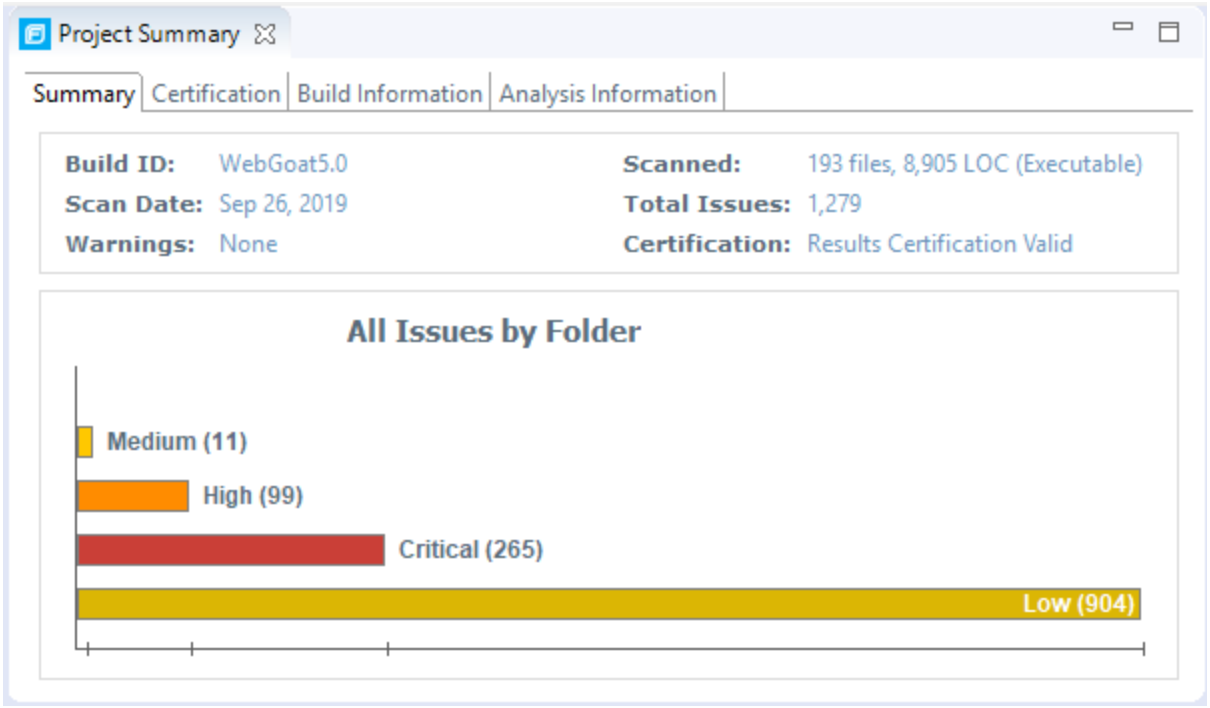
The following procedure uses the WebGoat sample Java application to demonstrate how to access information about sets of issues graphically depicted in the summary graph.

To access details about issue sets in an audit project:

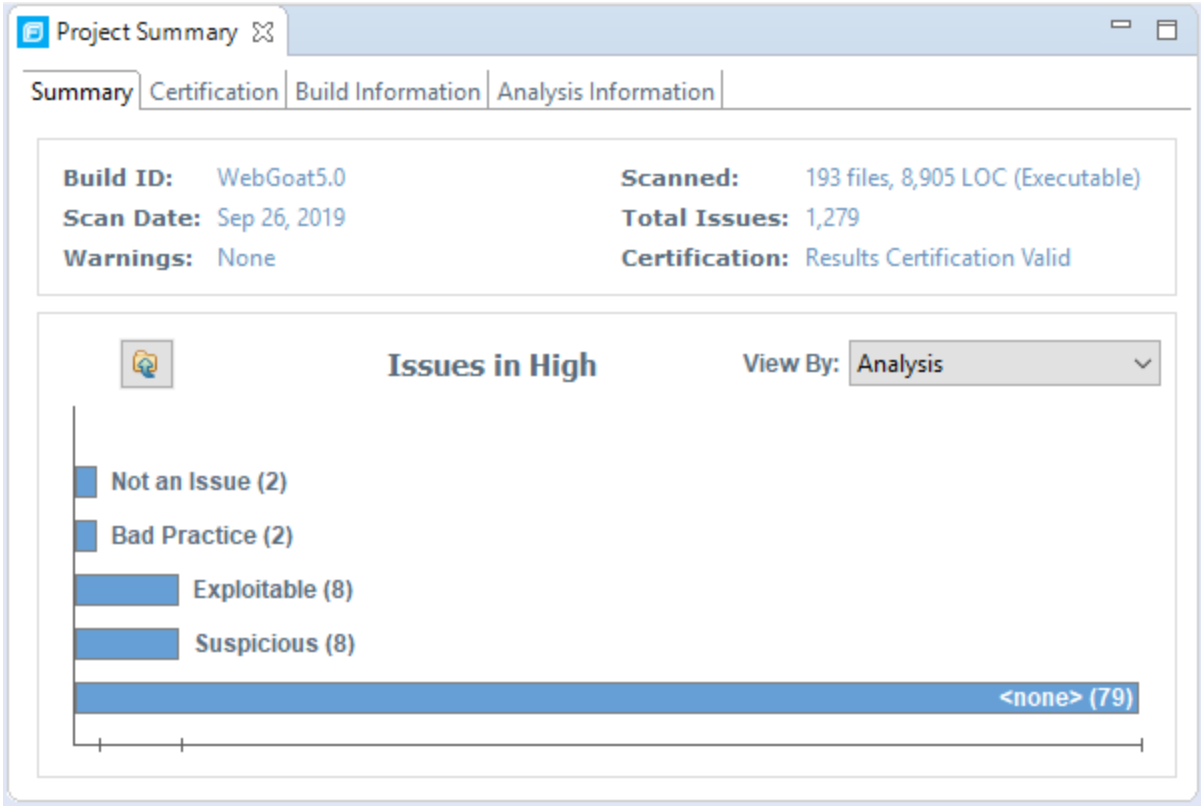
1. Scan your project source code or open an existing audit project.

   After the results are loaded, the **Project Summary** view displays the **Summary** tab, which includes the summary graph. The summary graph initially displays issues sorted into the **Critical**, **High**, **Medium**, and **Low** folders.

   Note: If you change the selection in the **Filter Set** list (**Static Analysis Results**), the summary graph changes accordingly.



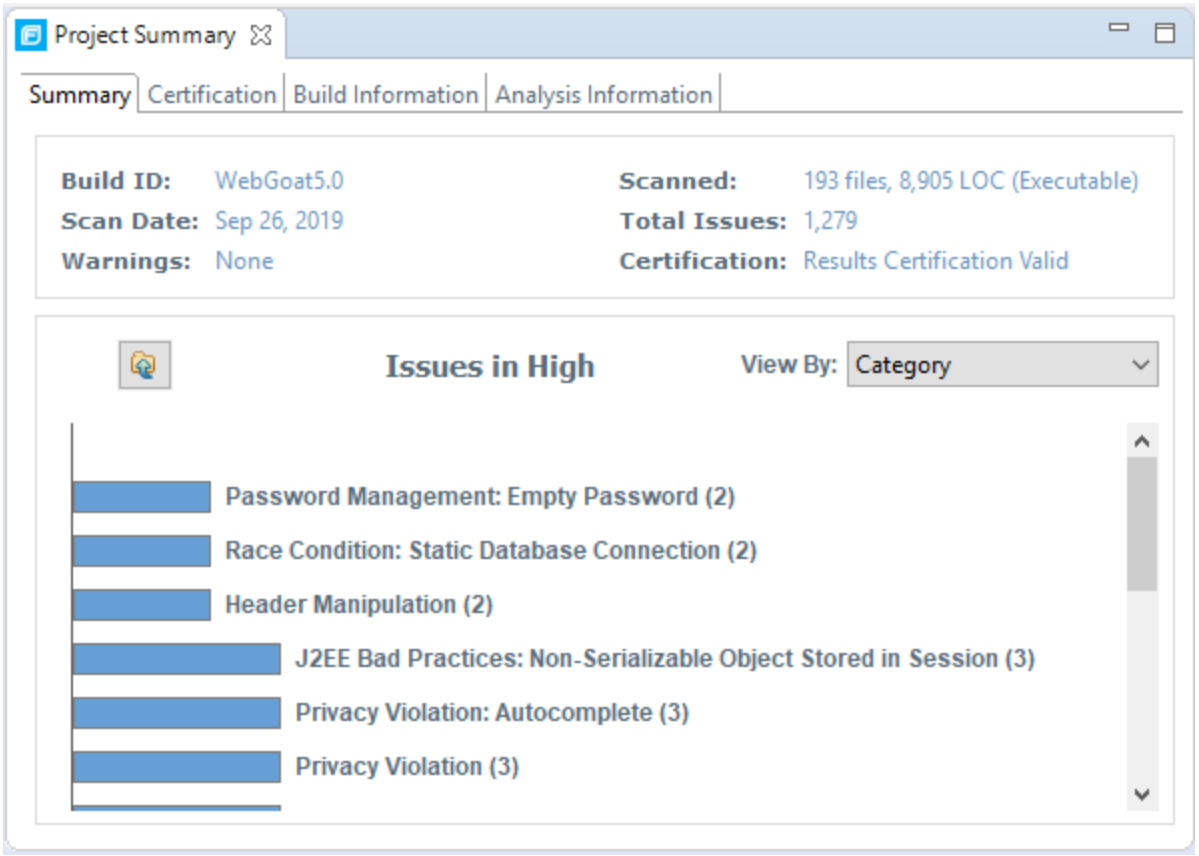
2. To see a different view of the high priority issues, click the **High** bar.



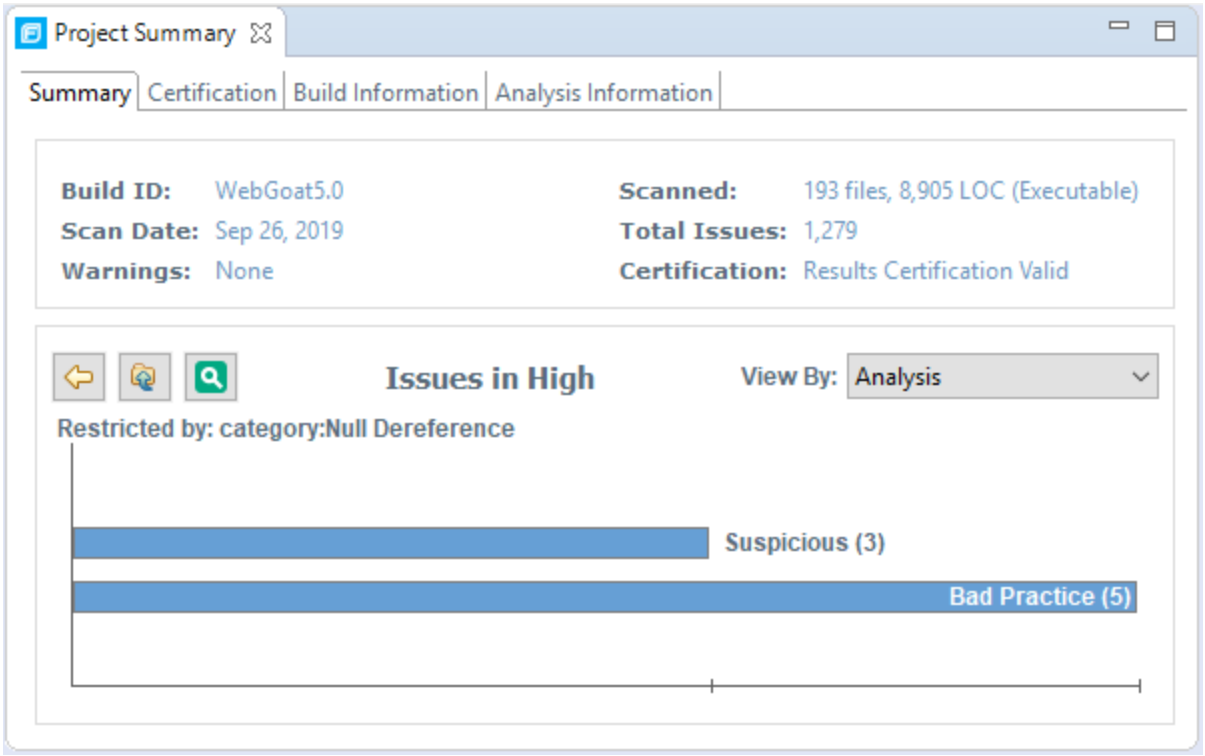
By default, the graph displays high priority issues based on the analysis attribute (assigned analysis values).

Note: The example here shows information for scan results that have been partially audited. If these results were from a fresh, unaudited scan, no analysis information would be available. The graph would just display a single bar that represents all (unaudited) high priority issues.

3. To view the high priority issues based on a different attribute, select an item from the **View By** list.

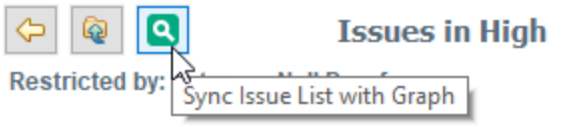


4. On the **Issues in High** bar graph, select a bar for a category that contains multiple issues.

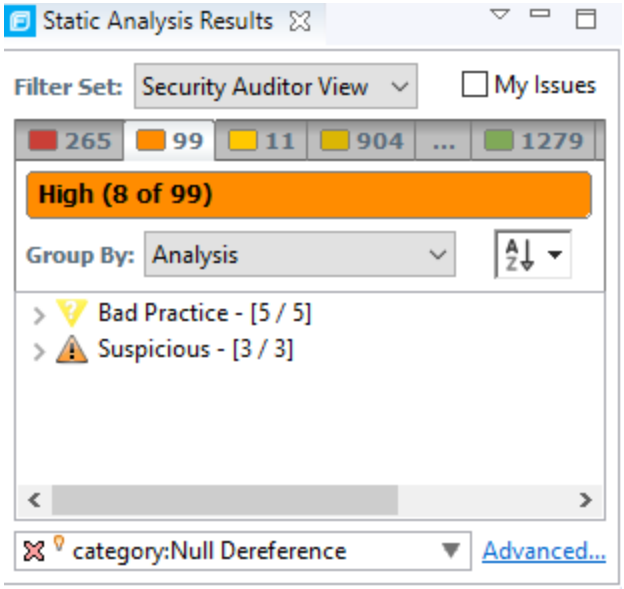


In the example shown here, the **Null Dereference** bar is selected. You can see that, of eight issues, three were marked as Suspicious and five were marked as Bad Practice.

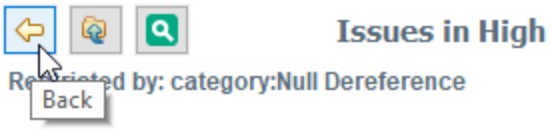
5. To synchronize the issues list with the displayed graphical view, click **Sync Issue List with Graph**.



The issues list in the **Static Analysis Results** view now reflects the selections in the summary graph.



6. To return to the previous view in the summary graph, click **Back**.



7. To return to the original summary graph view (issues based on priority), click **Return to Folder Graph**.

Analysis Trace View

When you select an issue, the **Analysis Trace** view displays the relevant trace output. 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 evidence is a presentation of the path that the tainted data follows from the source function to the sink function.

The Rule ID at the bottom of this panel provides the primary rule that found the issue.

Note: The Eclipse Remediation Plugin does not display the Rule ID.

For example, when you select an issue that is related to potentially tainted dataflow, the **Analysis Trace** view shows the direction the dataflow moves in this section of the source code.

The **Analysis Trace** view uses the icons listed 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 parameter to another in a function call
	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
	The execution jumps
	A branch is taken in the code execution
	A branch is not taken in the code execution
	Generic
	A runtime source, sink, or validation step

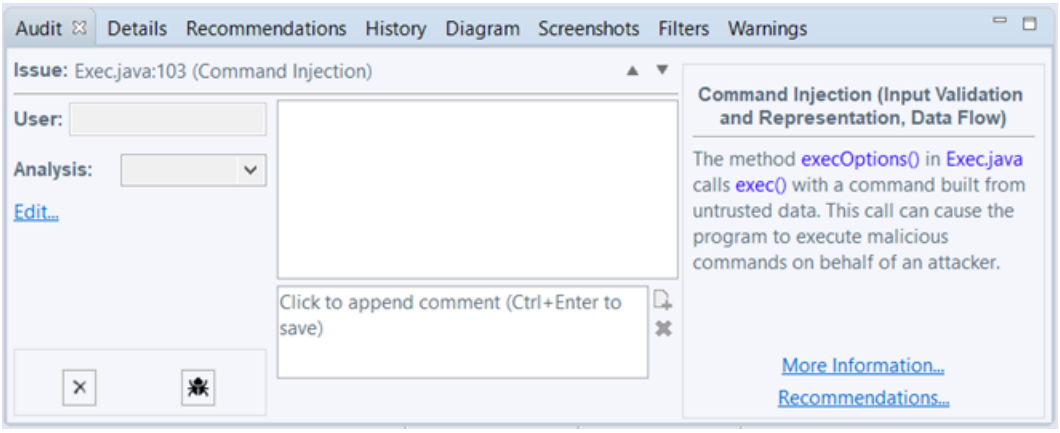
Icon	Description
	Taint change

The **Analysis Trace** view can display 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, and 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.

Issue Auditing View

The Issue Auditing view at the bottom center of the Fortify Audit perspective provides detailed information about each issue on the tabs described in the following topics.

Note: If any of the tabs are not visible, select **Window > Show View** to open them.



Audit Tab

The **Audit** tab displays information about the selected issue and enables auditors to add an audit evaluation, comments and custom tag values. The following table describes the tab elements.

Element	Description
Issue	Displays the issue location, including the file name and line number.
User	Displays the name of the user assigned to the issue if the results were uploaded to Micro Focus Fortify Software Security Center and a user was assigned in Fortify Software Security Center.
Analysis	List of values that the auditor can use to assess the issue. Valid values for **Analysis** are Not an Issue, Reliability Issue, Bad Practice, Suspicious, and Exploitable.

Element	Description
<custom_tags>	Displays any custom tags if defined for the audit project. If the audit results have been submitted to Audit Assistant in Fortify Software Security Center, then in addition to any other custom tags, the tab displays the following tags: • **AA_Prediction**—Exploitability level that Audit Assistant assigned to the issue. You cannot modify this tag value. • **AA_Confidence**—Confidence level from Audit Assistant for the accuracy of its **AA_Prediction** value. This is a percentage, expressed in values that range from 0.000 to 1.000. For example, a value of 0.982 indicates a confidence level of 98.2 percent. You cannot modify this tag value. • **AA_Training**—Whether to include or exclude the issue from Audit Assistant training. You can modify this value. For more information about Audit Assistant, see the *Micro Focus Fortify Software Security Center User Guide*.
Suppress	Suppresses the issue.
Unsuppress	Unsuppresses the issue (only visible if the issue is suppressed). Suppressed issues are hidden by default. To display suppressed issues, select **Options > Show Suppressed Issues**.
File Bug	Provides access to a supported bug tracker application.
Comment	Appends additional information about the issue to the comment field.
Rule Information	Shows information, such as the category and kingdom that describes the issue.
More Information	Opens the **Details** tab.
Recommendations	Opens the **Recommendations** tab.
Show merge conflicts	Shows merge conflicts in the **Comments** box that might exist after a merge of audit projects. This check box is available only if merge conflicts exist.

Details Tab

The **Details** tab provides a detailed description of the selected issue. The following table describes the tab elements.

Element	Description
Abstract/Custom Abstract	Summary description of the issue, including custom abstracts that your organization defined.
Explanation/Custom Explanation	Description of the conditions in which this type of issue occurs. This includes a discussion of the vulnerability, the constructs typically associated with it, how an attacker can exploit it, and the potential consequences of an attack. This element also provides custom explanations that your organization defined.
Instance ID	Unique identifier for the issue.
Priority Metadata Values	Includes impact and likelihood.
Legacy Priority Metadata Values	Includes severity and confidence.
Remediation Effort	The relative amount of effort required to fix and verify an issue.

WebInspect Agent Details Tab

The **WebInspect Agent Details** tab displays the following information about runtime issues that Fortify WebInspect Agent discovered. The following table describes the tab elements.

Element	Description
Request	Shows the path of the request, the referrer address, and the method.
Stack Trace	Shows the order of methods called during execution and line number information. Blue, clickable code links are only displayed for Fortify Static Code Analyzer-scanned code.

Recommendations Tab

The **Recommendations** tab displays suggestions and examples of how to secure the vulnerability or remedy the bad practice. The following table lists the elements on the tab.

Element	Description
Recommendations/Custom Recommendations	Recommendations for this type of issue, including examples, as well as custom recommendations that your organization defined.
Tips/Custom Tips	Tips for this type of issue, including any custom tips that your organization defined.

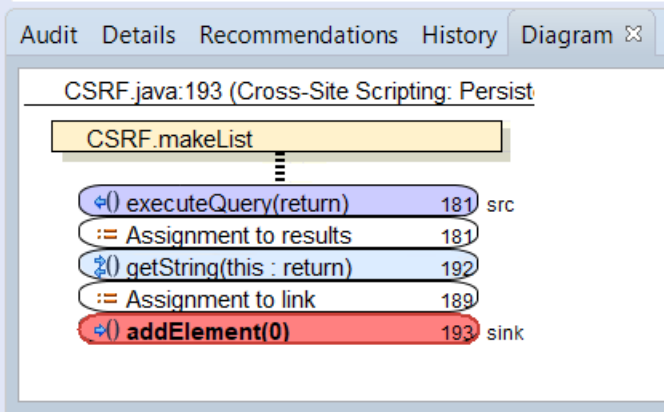
Element	Description
References/Custom References	Reference information, including any custom reference that your organization defined.

History Tab

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

Diagram Tab

The **Diagram** tab displays a graphical representation of the node execution order, call depth, and expression type of the issue selected in the **Static Analysis Results** view. This tab displays information that is relevant to the rule type. The vertical axis represents the execution order.



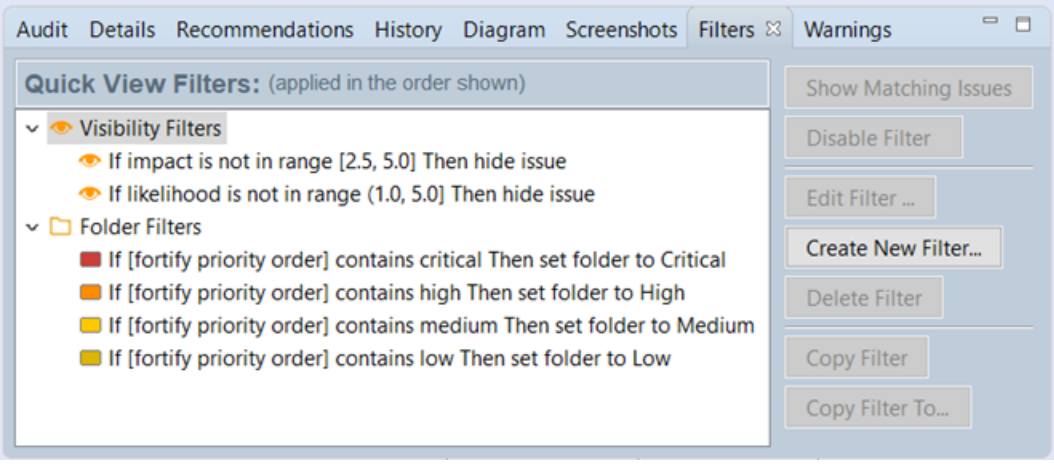
For dataflow issues, the trace starts with the first function to call the taint source, then traces the calls to the source (blue node), and ends the trace at the sink (red node). In the diagram, the source (src) and sink nodes are also labeled. A red X on a vertical axis indicates that the called function finished executing.

The horizontal axis shows the call depth. A line shows the direction that control is passed. If control passes with tainted data through a variable, then the line is red. If control passes without tainted data, the line is black.

The icons used for the expression type of each node in the diagram are the same icons used in the **Analysis Trace** view. To view the icons and the descriptions, see "Analysis Trace View" on page 41.

Filters Tab

The **Filters** tab displays all the filters in the selected filter set.

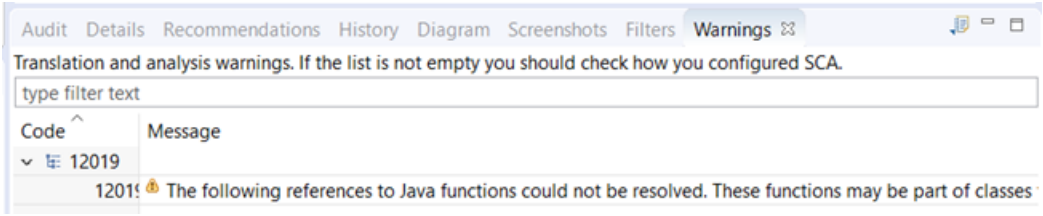


The following table describes the options to create new filters.

Option	Description
Filters	Displays a list of the visibility and folder filters configured in the selected filter set. • Visibility filters show or hide issues • Folder filters sort the issues into the folder tabs in the Static Analysis Results view Right-click a filter to show issues that match the filter or to enable, disable, copy, or delete it.
If	Displays the filters conditions. The first list displays a list of issue attributes, the second list specifies how to match the attribute, and third is the value the filter matches. **Note:** This option is visible when you create a new filter or edit an existing filter. In this case, a dialog box displays the **If** section.
Then	Indicates the filter type, where **Hide Issue** is a visibility filter and **Set Folder to** is a folder filter. **Note:** This option is visible when you create a new filter or edit an existing filter. In this case, a dialog box displays the **Then** section. For more information, see "Creating a Filter from the Issue Auditing View" on page 92.

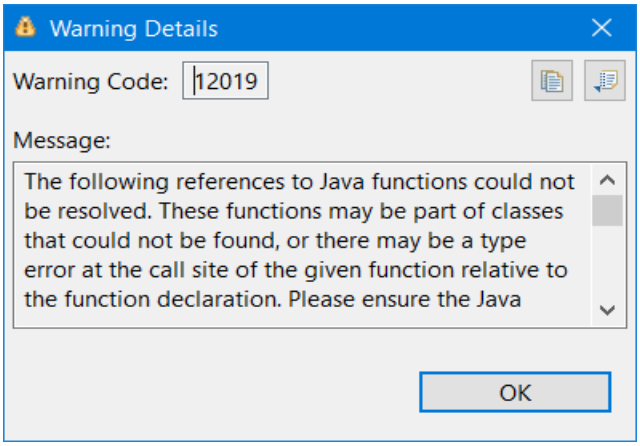
Warnings Tab

The **Warnings** tab lists any warnings that occurred during the analysis.



A common source of warnings are missing references. To resolve this type of warning, make sure that the reference files are either within the project directory structure or in a location known to Micro Focus Fortify Static Code Analyzer. The scan can also issue a warning if a class has no functional content. In this case, the warning is not an issue because an empty class has no impact on a scan.

The following table describes the **Warnings** tab options.

Task	Procedure
See the complete message that is truncated on the tab.	• Double-click the message. 
Copy a warning message to the clipboard.	• Right-click a message, and then select **Copy**.
Save a warning message to a file.	1. Right-click a message, and then select **Export Entry**. 2. Type a name for the file, and then click **Save**. The file includes the audit project name, FPR file location, the warning code, and the warning message.
Save all the warning messages to a file.	1. Click **Export Warnings**  . 2. Type a name for the file, and then click **Save**. The file includes the project name, FPR file location, the warning codes, and the warning messages.
Search the warning message	Type the search text in the filter text box.

Task	Procedure
Modify the text message at the top of the tab.	1. Edit the <*fortify_working_dir*>/config/tools/warnings-view.properties file where <*fortify_working_dir*> is: • Windows: C:\Users\<*username*>\AppData\Local\Fortify • Non-windows: /home/<*username*>/.fortify 2. Edit the text following message= to the text you want to display in the **Warnings** tab. Close and reopen the **Warnings** tab to see the updated text.

Viewing Issues in the Source Code

The source code editor shows the section of code related to the issue selected in the **Static Analysis Results** view. Each time you select an issue in the **Static Analysis Results** view, a tab opens in the source code editor and displays the code associated with the selected issue.

If multiple nodes represent an issue in the **Analysis Trace** view, the source code editor shows the code associated with the selected node.

Working with Issues

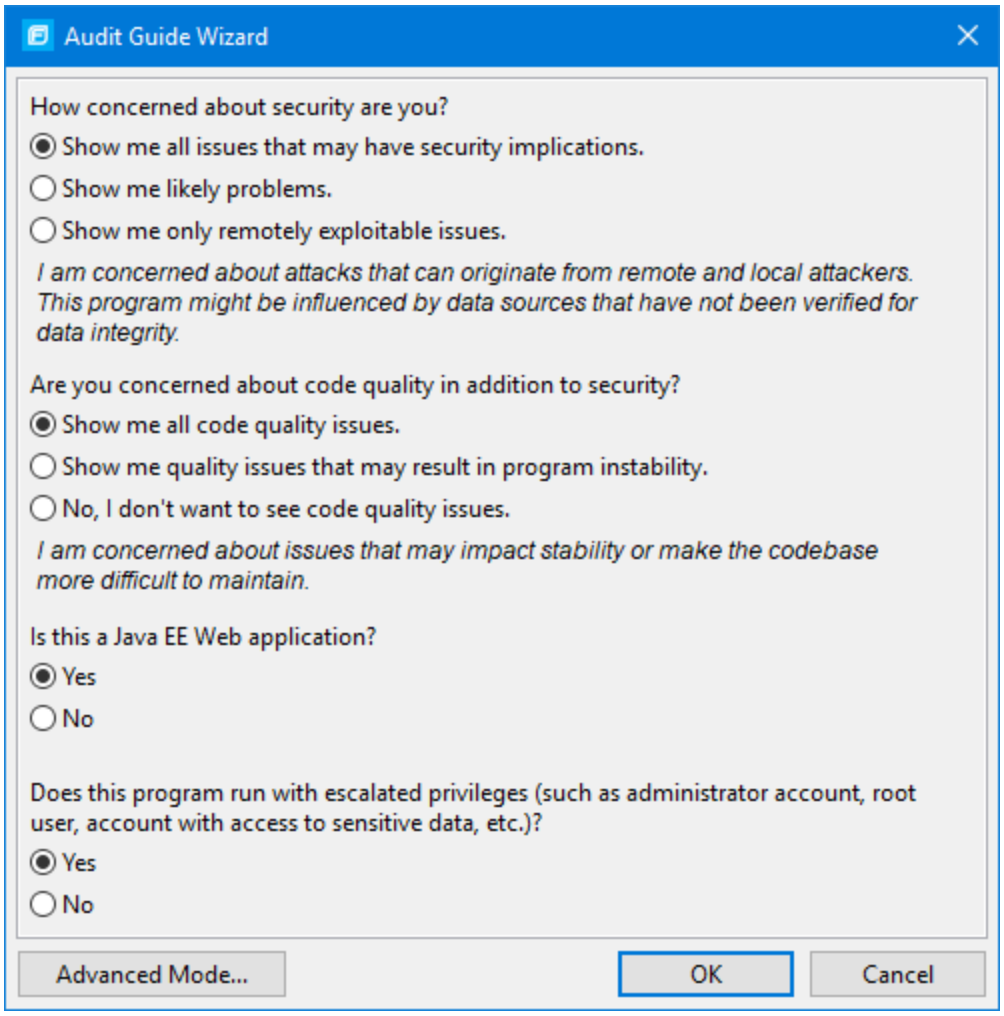
This section provides information about how to use the Eclipse Complete Plugin to review issues.

Filtering Issues with Audit Guide

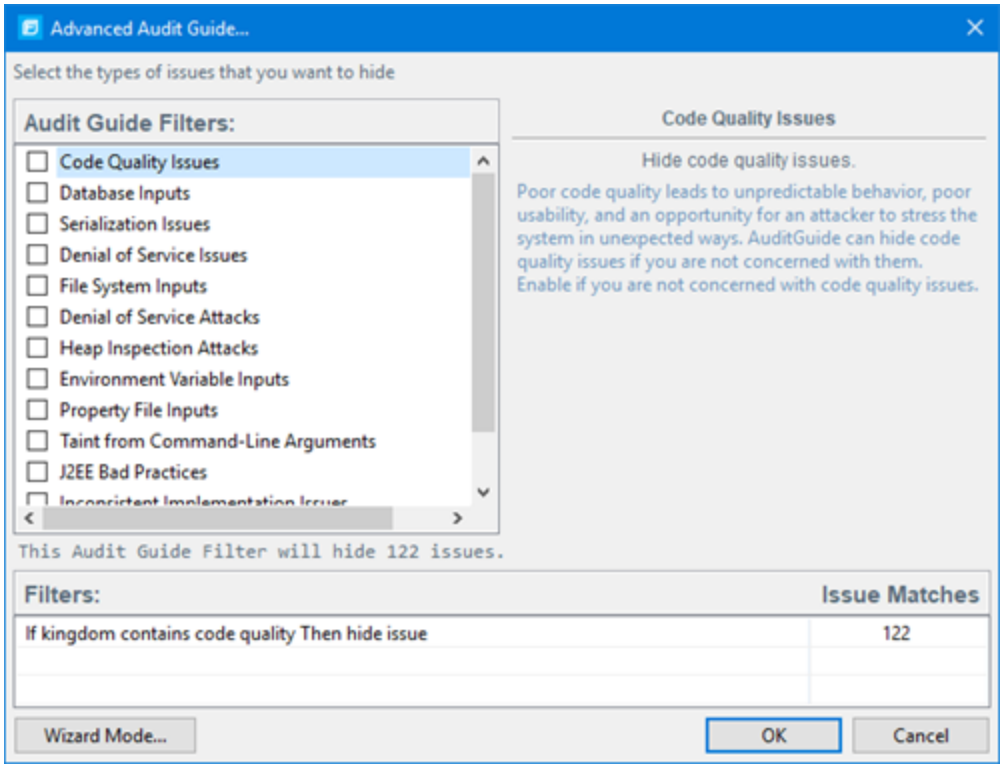
You can use the Audit Guide Wizard to filter vulnerability issues in your audit project based on a set of security-related questions.

To use the Audit Guide:

1. Select **Fortify > Audit Guide**.



2. Make your selections for the types of issues you want to display.
3. To use the advanced filter options, click **Advanced Mode**.
   The Advanced Audit Guide dialog box opens.



a. In the **Audit Guide Filters** list, select the types of issues you want to filter out and ignore.

   As you select items in the **Audit Guide Filters** list, the Audit Guide Wizard also displays the filter details for the selected filter type in the **Filters** table, including the number of issues that match each filter.

b. To see a description of an issue type, click its name in the **Audit Guide Filters** list.

   The Audit Guide Wizard displays a description to the right of the list.

4. Click **OK** to apply your filter selections.

Grouping Issues

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

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

You can view issues with any of the **Group By** options, and you can create and edit customized groups. The **Group By** options enable you to group and view the issues in different ways. In practice, you will probably switch frequently between different groupings. The following table lists descriptions of the standard Group By options.

Option	Description
Analysis	Groups issues by the audit analysis, such as Suspicious, Exploitable, and Not an Issue.
Analysis Type	Groups issues by analyzer product, such as SCA, WEBINSPECT, and SECURITYSCOPE (WebInspect Agent).
Analyzer	Groups issues by analyzer group, such as Control Flow, Data Flow, Findbugs, Pentest, and Structural.
App Defender Protected	Groups issues by whether Application Defender can protect the vulnerability category.
Category	Groups issues by vulnerability category. This is the default setting.
Category Analyzer	A custom group that groups issues by category and then by analyzer.
Correlated	Groups issues by whether the issue is related directly or indirectly with an issue uncovered by another analyzer.
Correlation Group	Groups issues that are correlated with each other.
File Name	Groups issues by file name.
Fortify Priority Order	Groups issues as Critical, High, Medium, and Low based on the analyzer's combined values of impact and likelihood.
Kingdom	Groups issues by the Seven Pernicious Kingdoms classification.
Manual	Groups issues by whether they were manually created by penetration test tools, and not automatically produced by a web crawler such as Fortify WebInspect.
New Issue	Shows which issues are new since the last scan. For example, if you run a new scan, any issues that are new display in the tree under the **New Issues** group and the others are displayed in the **Issue Updated** group. Issues not found in the latest scan are displayed in the **Removed** list.
<*metadata_listname*>	Groups issues by the alternative metadata external list names (for example, OWASP Top 10 <*year*>, CWE, PCI <*version*>, STIG <*version*>, and so on).
Package	Groups issues by package or namespace. Does not appear for projects to which this option does not apply, such as C projects.

Option	Description
Priority by Category	A custom group that groups issues by Fortify Priority Order and then by category.
Sink	Groups issues that share the same dataflow sink function.
Source	Groups issues that share the same dataflow source functions.
Source File Type	Groups issues by source file types Micro Focus Fortify Static Code Analyzer recognizes. **Note:** Issues in files with different file extensions that are the same source file type are grouped together (for example, issues in files with the extensions: `html`, `htm`, and `xhtml` are grouped under html).
Taint Flag	Groups issues by the taint flags that they contain.
<none>	Displays a flat view without any grouping.
Edit	Select **Edit** to create a custom Group By option.

The following table describes additional grouping options that are available when you create a custom Group By option (see "Creating a Custom Group By Option" below).

Option	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.
Primary Context	Groups issues where the primary location or sink node function call occurs in the same code context.
Source Context	Groups dataflow issues that have the source function call contained in the same code context.
Status	Groups issues by the audit status (Reviewed, Unreviewed, or Under Review)
URL	Groups dynamic issues by the request URL.

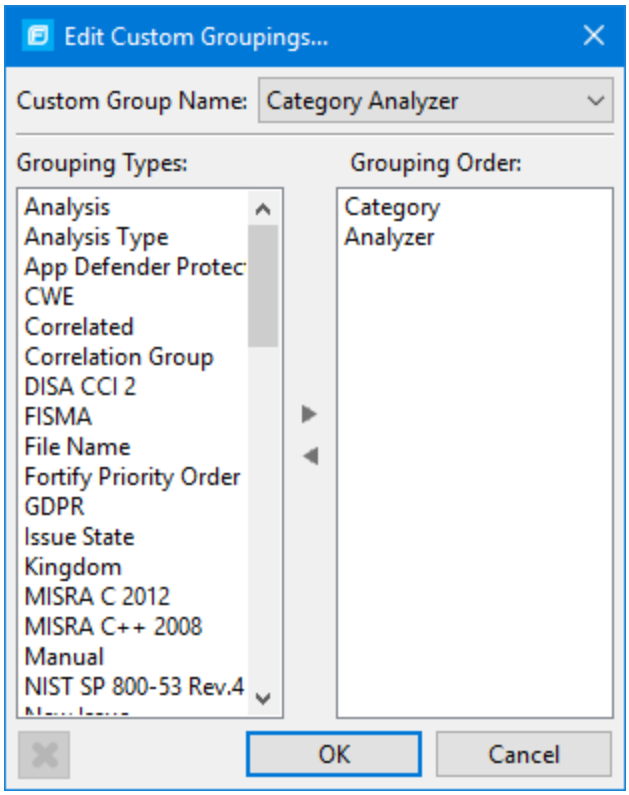
Creating a Custom Group By Option

You can create a custom Group By option that groups issues in a hierarchical format in sequential order based on specific attributes.

To create a new grouping option:

1. In the **Group By** list, select **Edit**.

   The Edit Custom Groupings dialog box opens.



2. To create a custom group by option, do the following:
   a. Select **Create New** from the **Custom Group Name** list.
   b. In the Enter Value dialog box, type a name for the new custom group.
   c. Click **OK**.
3. From the **Grouping Types** list on the left, select a grouping type, and then click the right arrow to move the option to the **Grouping Order** column.

   For example, selecting **Category** and then **Analyzer** creates a list that has top-level nodes that contain the category of the issue, such as Buffer Overflow, with the issues grouped below by analyzer (such as semantic, or dataflow), followed by the issues.

   ```
   -Buffer Overflow [0/2]
   --DataFlow [0/1]
   ----Main.cs:234
   -+Semantic [0/1]
   ```
4. Repeat step 3 to select additional grouping types.
5. To change the order of the grouping types:
   a. In the **Grouping Order** list, select the grouping type that you want to move up or down in the grouping order.
   b. Right-click the selected grouping type, and then select **Move Up** or **Move Down** from the

shortcut menu.

6. To delete a custom grouping, click **Delete**  .

Evaluating Issues

To evaluate and assign audit values to an issue or group of issues:

1. Select the issue or group of issues in the **Static Analysis Results** view, see "About Viewing Scan Results" on page 30.
2. In the Issue Auditing view, read the abstract on the **Audit** tab. This abstract provides high-level information about the issue, such as the analyzer that found the issue.

   For example, `Command Injection (Input Validation and Representation, dataflow)` indicates that this issue that the Dataflow Analyzer detected, is a Command Injection issue in the Input Validation and Representation kingdom.
3. Click the **More Information** link to get more details about the issue.
4. On the **Audit** tab, specify an Analysis value for the issue to represent your evaluation.
5. Specify values for any custom tags as your organization requires.

   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, you can click to select a date from a calendar.
6. If the audit results have been submitted to Audit Assistant in Micro Focus Fortify Software Security Center, then you can specify whether to include or exclude the issue from Audit Assistant training from the **AA_Training** list.

   Note: If you select a different value for **Analysis** than the **AA_Prediction** value set by Audit Assistant, and you select **Include** from the **AA_Training** list, then the next time the data is submitted to Audit Assistant, it updates the information used to predict whether an issue represents a true vulnerability. For more information about Audit Assistant, see the *Micro Focus Fortify Software Security Center User Guide*.
7. (Optional) In the **Comments** box, type comments relevant to the issue and your evaluation.

Performing Quick Audits

As you audit issues, you can use a keyboard combination to assign an analysis value to multiple selected issues.

To assign an analysis value to multiple issues simultaneously:

1. In the **Static Analysis Results** view, select the issues to which you want to assign the same analysis value.
2. Press **Ctrl** + **Shift** + **A** (**Cmd** + **Shift** + **A** on macOS).

   The Eclipse Complete Plugin displays a window in the lower-right corner to indicate you are in **Quick Audit Issue** mode.

Note: Do not hold this keyboard combination in the next step.

3. Press one of the following number keys:
   - To assign Not an Issue, press **1**
   - To assign Reliability Issue, press **2**
   - To assign Bad Practice, press **3**
   - To assign Suspicious, press **4**
   - To assign Exploitable, press **5**
   - To assign a custom analysis value configured for your organization, press the number that corresponds to its position in the **Analysis** list on the **Audit** tab.

Shortcuts are provided for only the first ten values in the **Analysis** list. (To assign the tenth value in the list, you press **Ctrl** + **Shift** + **A**, and then press **0**). If no value is listed for the key you press, no value is assigned.

Performing Quick Audits for Custom Tags

Instead of using the Analysis tag for quick audits, you can use a custom tag your organization has created.

To use a custom tag for quick audits:

1. Select **Fortify > Options**.
2. In the left panel, select **Audit Configuration**, and then click the **Configuration** tab on the right.
3. Under **Quick Audit Preference**, from the **Attribute to use for quick action audit** list, select a custom tag.

   Note: Only list-type tags are available to use for quick audits.

   If no custom tags have been created, the list only includes the **Analysis** tag.
4. Click **OK**.

The keyboard shortcut functions just as it does for the Analysis tag values. Shortcuts are provided for only the first ten values in the list of custom tag values. (To assign the tenth value in the list, you press **Ctrl** + **Shift** + **A**, and then press **0**). If there is no value in the list for the key you press, no value is assigned.

For information about custom tags, see "Configuring Custom Tags for Auditing" on page 98.

Adding Screen Captures to Issues

You can attach a screen shot or other image to an issue. Attached images are stored in the FPR file and are accessible from Micro Focus Fortify Software Security Center. The following image formats are supported:

- GIF
- JPG

- PNG

To add an image to an issue:

1. Select the issue.
2. In the Issue Auditing panel, click the **Screenshots** tab.
3. Click **Add**.
   The New Screenshot dialog box opens.
4. Browse to and select the image file.
5. (Optional) In the **Description** box, type a description.
6. Click **Add**.

Viewing Images

After you add an image to an issue, the image is displayed on the right side of the **Screenshots** tab.

To view a full-size version and complete description of an image added to an issue:

1. In the Issue Auditing Panel, click the **Screenshots** tab.
2. In the list, click an image to view.
3. Click **Preview**.

Creating Issues for Undetected Vulnerabilities

Add undetected issues that you want to identify as issues to the issues list. You can audit manually configured issues on the **Audit** tab, just as you do other issues.

To create an issue:

1. Select the object in the line of code in the source code tab.
2. Right-click the line that contains the issue, and then select **Create New Issue**.
   The Create New Issue dialog box opens.
3. Select the issue category, and then click **OK**.

The issues list displays the file name and source code line number for the new issue next to a blue icon.
The rule information in the **Audit** tab includes `Custom Issue`. You can edit the issue to include audit information, just as you can other issues.

Suppressing Issues

You can suppress issues that are either fixed or that you do not plan to fix.

To suppress an issue, do one of the following:

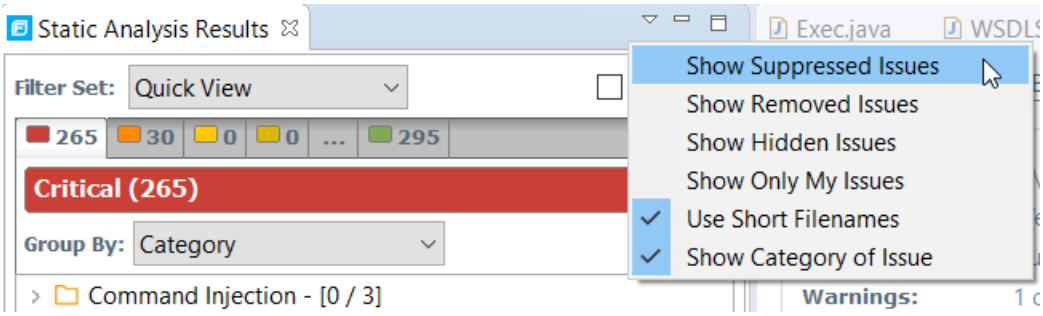
- In the **Static Analysis Results** view, select the issue, and then, on the **Audit** tab in the Issue Auditing view, click **Suppress** .

- In the **Static Analysis Results** view, right-click the issue, and then click **Suppress Issue**.

Note: You can select and suppress multiple issues at the same time.

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 review results that have been suppressed, select **Show Suppressed Issues** from the **View** menu on the **Static Analysis Results** toolbar.



To unsuppress an issue, first display the suppressed issues and then do one of the following:

- In the **Static Analysis Results** view, select the suppressed issue, and then, on the **Audit** tab in the Issue Auditing view, click **Unsuppress** .
- Right-click the issue in the **Static Analysis Results** view, and then select **Unsuppress Issue**.

Note: You can select and unsuppress multiple issues at the same time.

Creating Attribute Summary Tables for Multiple Issues

You can create a summary table of attributes (for example, in spreadsheet software such as Excel or Google Sheets) for any number of issues that you select from the **Static Analysis Results** view. You specify the format options, select the issues, and then paste the comma delimited data into a spreadsheet program to create the summary table.

The table can contain an attributes column followed by a single values column for every issue selected or, the table can display one row per attribute and its corresponding values. Alternatively, you can specify a customized table layout for the values that you copy to your spreadsheet program.

To create a spreadsheet table that contains an attributes column followed by a single values column for each selected issue:

1. Select **Fortify > Options**.
2. In the left panel, select **Audit Configuration**, and then select the **Configuration** tab.
3. Under **Multiple Issues Copy Format**, leave the **[h] List issues in columns** option selected.
4. Select the attributes you want to include from the **Include immutable attributes**, **Include mutable attributes**, and **Include custom tags** check boxes.
5. Click **OK**.

6. From the **Static Analysis Results** view, use the **Ctrl** or **Shift** key and select all the issues you want to include in a table.
7. With the issues selected, press **Ctrl** + **Alt** + **Shift** + **C**.
8. Start the spreadsheet software, and then paste (**Ctrl** + **V**) the copied data into a single column.

To create a spreadsheet table that displays one row per attribute and its values:

1. Select **Fortify > Options**.
2. In the left panel, select **Audit Configuration**, and then select the **Configuration** tab.
3. Under **Multiple Issues Copy Format**, select the **[v] List issues in rows** option.
4. Select the attributes you want to include from the **Include immutable attributes**, **Include mutable attributes**, and **Include custom tags** check boxes.
5. Click **OK**.
6. From the **Static Analysis Results** view, use the **Ctrl** or **Shift** key and select all the issues you want to include in a table.
7. With the issues selected, press **Ctrl** + **Alt** + **Shift** + **C**.
8. Start the spreadsheet software, and then paste (**Ctrl** + **V**) the copied data into a single column.

To create a customized table layout for the values that you copy to a spreadsheet program:

1. Select **Fortify > Options**.
2. In the left panel, select **Audit Configuration**, and then select the **Configuration** tab.
3. Under **Multiple Issues Copy Format**, select the **Format manually** option.
4. In the **Attribute value format** box, use the string described in the following table to specify the data layout, format, and separators for the values you want to copy.

String	Function
`[h]`	Columnar format - Attributes are inserted in a single column and the spreadsheet table expands to the right (horizontally) with a new column added for each issue copied in.
`[v]`	Row format - Attributes are inserted in a single row (table header) and a new row populated with values is added for each issue added (table expands vertically).
`%s`	Textual data (you can use the complete `java.util.Formatter` syntax). See the `java.util.Formatter` documentation at https://docs.oracle.com/javase/8/docs/api/java/util/Formatter.html.
`,` `;` or tab	Separator symbol - To import the copied value into most spreadsheet programs, you must specify the separator to use in the format field.
`'...'`	Apply the preceding format string to all elements in the selection. This is only valid if the format specification starts with `[h]` or `[v]`.

String	Function
%n	Line separator (platform independent), whether it is the last value for an issue in a row formatted table `[v]` or it is the last value of a given attribute in a columnar formatted table `[h]`.

For example, to specify which specific attributes you want to copy with the row format (`[v]`), use `[v]%file$s,%category$s,%fortify priority order$s%n`. This copies the three attributes for each selected issue.

5. To see the result of your syntax, look under **Result example**.

   The example shown changes as you change the value in the **Attribute Value Format** box.

   Note: Examples are not available for complex manual formats.

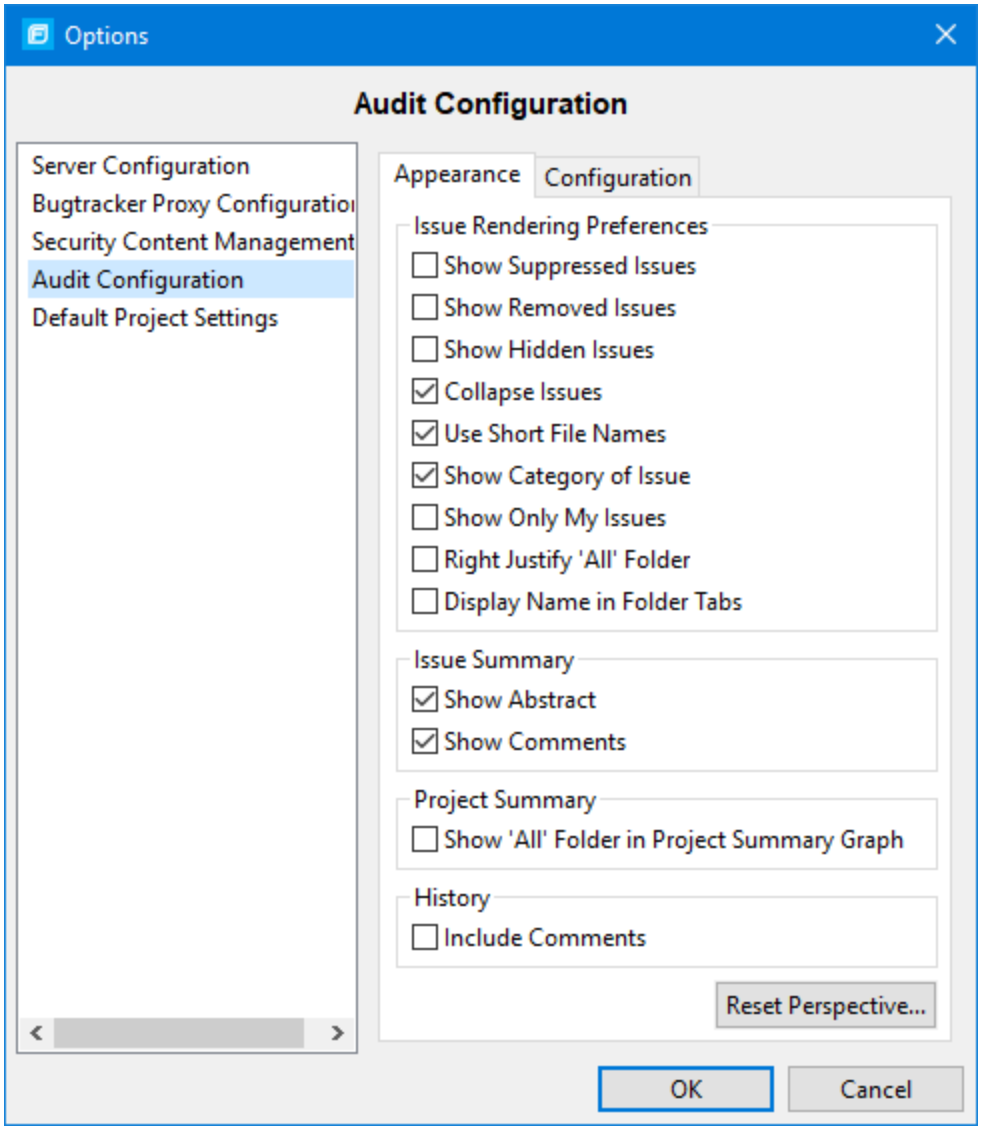
6. Select the attributes you want to include from the **Include immutable attributes**, **Include mutable attributes**, and **Include custom tags** check boxes.
7. Click **OK**.

Customizing the Static Analysis Results View

You can customize the **Static Analysis Results** view to determine which issues it displays.

To change the **Static Analysis Results** view:

1. Select **Fortify > Options**.
2. In the left panel, select **Audit Configuration**.



3. To change your preferences on the **Appearance** tab, select or clear the check boxes described in the following table.

Preference	Description
Show Suppressed Issues	Displays all suppressed issues (disabled by default).
Show Removed Issues	Displays all issues that were uncovered in the previous analysis, but are no longer evident in the new **Static Analysis Results** view. When multiple scans are run on a project over time, vulnerabilities are often remediated or become obsolete. Micro Focus Fortify Static Code Analyzer marks these vulnerabilities as Removed Issues.
Show Hidden Issues	Displays all hidden issues.

Preference	Description
Collapse Issues	Shows similar issues based on certain attributes under a shared parent node in the **Static Analysis Results** view.
Use Short File Names	References the issues in the **Static Analysis Results** view by file name only, instead of by relative path.
Show Category of Issue	Displays the category of an issue in the **Static Analysis Results** view and the **Audit** tab.
Show Only My Issues	Displays only issues assigned to you.
Right justify 'All' Folder	Displays the **All** folder aligned on the right.
Display Name in Folder Tabs	Displays the name text in the folder tabs.
Show Abstract	Displays the abstract text in the **Audit** tab..
Show Comments	Displays comments in the **Audit** tab.
Show 'All' Folder in Project Summary Graph	Displays another bar in the chart on the **Summary** tab in the **Project Summary** view.
Include Comments	Displays the history items for comments on the **History** tab.

Note: To restore the default settings at any time, click **Reset Perspective**.

4. To save your preferences, click **OK**.

Submitting an Issue as a Bug

You can submit issues to your bug tracker application if you have integrated the application with Eclipse or if you are using Micro Focus Fortify Software Security Center.

To submit an issue as a bug:

1. Select the issue in the **Static Analysis Results** view, and then, on the **Audit** tab, click **File Bug** .
   When you submit a bug for first time, the Configure Bugtracker Integration dialog box opens. (For information about configuring the plugin with bug tracker applications, see "Integrating with a Bug Tracker Application" on the next page.) Select a bug tracker application, and then click **OK**.
2. Specify all required values and review the issue description. Depending on the integration and your bug tracker application, the values include items such as the bug tracker application URL, product name, severity level, summary, and version.
3. If the connection to the bug tracker requires a proxy, select the **Use proxy** check box.

With this option selected, the Fortify Plugins for Eclipse use the proxy settings specified for bug trackers. For more information, see "Configuring Proxy Settings for Bug Tracker Integration" below.

4. Click **Submit**.

You must already be logged on before you can file a bug through the user interface for bug tracker applications that require a logon. The issue is submitted as a bug in the bug tracker application.

If you use Fortify Software Security Center, you can submit an issue as a bug using a bug tracker application configured through Fortify Software Security Center.

To submit an issue as a bug through Fortify Software Security Center:

1. Select the issue in the **Static Analysis Results** view, and then, on the **Audit** tab, click the **File Bug** icon.

   When you submit a bug for first time, the Configure Bugtracker Integration dialog box opens. Select **Fortify Software Security Center**, and then click **OK**.
2. Specify the values if changes are needed and review the issue description. Depending on the integration and your bug tracker application, the values include items such as the bug tracker application URL, product name, severity level, summary, and version.
3. Click **Submit**.

If your bug tracker application requires you to log on, you must do so before you can file a bug through that interface.

Integrating with a Bug Tracker Application

The Eclipse Complete Plugin provides a plugin interface to integrate with bug tracker applications. This enables you to file bugs directly from the Eclipse Complete Plugin. For a list of supported bug tracker applications, see the *Micro Focus Fortify Software System Requirements* document.

To select the plugin to use:

1. Open an audit project.
2. Select **Fortify > Configure Bugtracker**.

Note: For Jira bug tracker integration, you must restart Eclipse after you change the proxy settings.

If installed with Fortify SCA and Applications, example source code for bug tracker plugins is available in `<sca_install_dir>/Samples/advanced/BugTrackerPlugin<bugtracker>`, where *<bugtracker>* is the name of the bug tracker application.

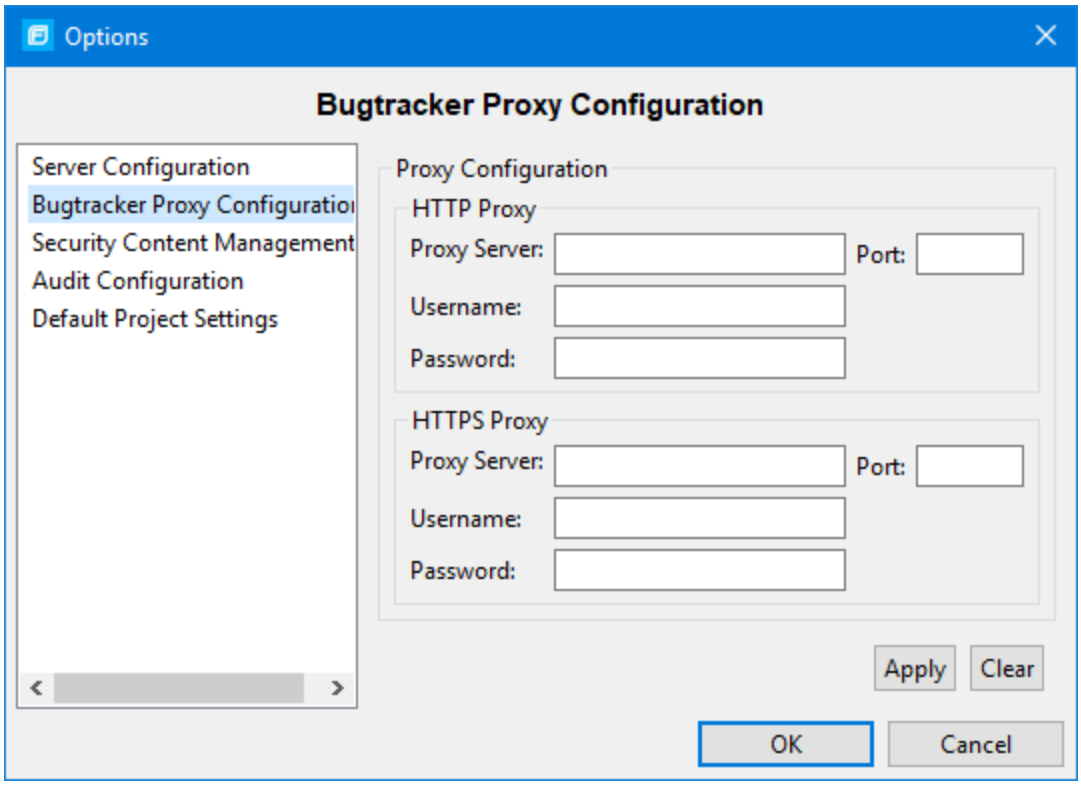
To write your own plugin, see the instructions in the `README` text file, which is in each bug tracker directory. Information about the API is included in the JavaDoc located in `<sca_install_dir>/Samples/advanced/JavaDoc/public-api/index.html`.

Configuring Proxy Settings for Bug Tracker Integration

If the bug tracker you use requires a proxy connection, specify the proxy settings. When you submit an issue as a bug, select the **Use proxy** check box. The Fortify Plugins for Eclipse provide the proxy settings to the bug tracker plugin.

To configure proxy settings for bug tracker integration:

1. Select **Fortify > Options**.
2. In the left panel, select **Bugtracker Proxy Configuration**.



3. Under **HTTP Proxy**, specify the proxy server, port number, and optionally credentials for proxy authentication.
4. If the connection uses HTTPS requests, then provide the proxy settings under **HTTPS Proxy**.
5. Click **OK** to save your changes.

Searching for Issues

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

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 the term is wrapped in quotation marks (" ")

Comparison	Description
regex	Searches for values that match a Java-style regular expression delimited by a forward slash (/) Example: `/eas.+?/` **Note:** This comparison is not available in the remediation plugins.
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 string 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 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.

For more information, see "Search Modifiers" below.

Search Modifiers

You can use a search modifier to specify to which attribute of an issue the search term applies.

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

A search that is not qualified by a modifier tries to match the search string on the following 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 result that contains the specified string.
- To apply the search to a specific modifier, type the modifier name and the string as follows: `analyzer:control flow`. This returns all results whose analyzer is `control flow`.

The following table describes the search modifiers. A few modifiers have a shortened modifier name indicated in parentheses. 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 by analyzer product such as `SCA` and `WEBINSPECT`.
`analyzer`	Searches the issues for the specified analyzer such as `control flow`, `data flow`, `structural`, and so on.
`[app defender protected]` (`def`)	Searches for issues based on whether Application Defender can protect the vulnerability category (`protected` or `not protected`).
`[attack payload]`	Searches for issues that contain the search term in the part of the request that caused the vulnerability for penetration test results.
`[attack type]`	Searches for issues based on the type of penetration test attack conducted (URL, parameter, header, or cookie).
`audience`	Searches for issues based on intended audience such as `dev`, `targeted`, `medium`, `broad`, and so on.
`audited`	Searches the issues to find `true` if the primary custom tag is set and `false` if the primary custom tag is not set. The default primary tag is the Analysis tag.
`body`	Searches for issues that contain the search term in the HTTP message body in penetration test results, which is all the data that is transmitted immediately following the headers.
`bug`	Searches for issues that contain the search term in the information for the filed bug.

Search Modifier	Description
	Note: This information is discarded each time you restart Eclipse.
`category(cat)`	Searches for the specified category or category substring.
`class`	Searches for issues based on the specified class name.
`comments (comment, com)`	Searches for issues that contain the search term in the comments that have been submitted on the issue.
`commentuser`	Searches for issues with comments from a specified user.
`confidence (con)`	Searches for issues that have the specified confidence value (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 another analyzer.
`[correlation group]`	Searches for issues based on whether the issues are in the same correlation group.
`dynamic`	Searches for issues that have the specified dynamic hot spot ranking value.
`file`	Searches for issues where the primary location or sink node function call occurs in the specified file.
`filetype`	Searches for issues based on the file type such as `asp`, `csharp`, `java`, `jsp`, `xml`, and so on.
`[fortify priority order]`	Searches for issues that have a priority level that matches the specified priority determined by Micro Focus Fortify Static Code Analyzer. Valid values are `critical`, `high`, `medium`, and `low`, based on the expected *impact* and *likelihood* of exploitation. The impact value indicates the potential damage that might result if an issue is successfully exploited. The likelihood value is a combination of confidence, accuracy of the rule, and probability that an attacker can exploit the issue.

Search Modifier	Description
`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 70.
`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 (SCA, WebInspect, and WebInspect Agent).
`maxconf`	Searches for all issues that have a confidence value equal to or less than the number specified as the search term.
`maxVirtConf`	Searches for dataflow issues that have a virtual call confidence value equal to or less than the number specified as the search

Search Modifier	Description
	term.
`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.
`[primary context]`	Searches for issues where the primary location or sink node function call occurs in the specified code context. Also see sink and [source context].
`primaryrule (rule)`	Searches for all issues related to the specified sink rule.
`probability`	Searches for issues based on the probability value specified (1.0 through 5.0).
`[remediation effort]`	Searches for issues based on the remediation effort value specified. The valid values are whole numbers from 1.0 to 12.0.
`[request id]`	This attribute is not currently used.
`response`	Searches for issues that contain the search term in the response from the protocol used in penetration test results.
`ruleid`	Searches for all issues reported by the specified rule IDs used to generate the issue source, sink and all passthroughs.
`[secondary requests]`	This attribute is not currently used.

Search Modifier	Description
`severity (sev)`	Searches for issues based on the specified severity value (legacy metadata).
`sink`	Searches for issues that have the specified sink function name. Also see [primary context].
`source`	Searches for dataflow issues that have the specified source function name. Also see [source context].
`[source context]`	Searches for dataflow issues that have the source function call contained in the specified code context. Also see source and [primary context].
`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. Also see "line" on page 68.
`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.
`trace`	Searches for issues that have the specified string in the dataflow trace. **Note:** This search modifier is not available in the remediation plugin.
`tracenode`	Enables you to search on the nodes within an issue's analysis trace. Each tracenode search value is a concatenation of the tracenode's file path, line number, and additional information. **Note:** This search modifier is not available in the remediation plugin.
`tracenodeAllPaths`	Searches for the specified value in all the steps of analysis trace evidence.

Search Modifier	Description
	Note: This search modifier is not available in the remediation plugin.
`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.
<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 a date-type custom tag, specify the date in the format: yyyy-mm-dd.
<metadata_listname>	Searches for issues based on the value of the specified metadata external list. Metadata external lists include `CWE`, `FISMA`, `[OWASP top 10 <year>]`, `[PCI <version>]`, `[STIG <version>]`, and others.

Search Query Examples

The following are search query examples that use search modifiers.

- To search for all privacy violations in file names that contain `jsp` with `getSSN()` as a source, type:
  `category:"privacy violation" source:getssn file:jsp`
- To search for all file names that contain `com/fortify/awb`, type:
  `file:com/fortify/awb`
- To search for all paths that contain traces with `mydbcode.sqlcleanse` as part of the name, type:
  `trace:mydbcode.sqlcleanse`
- To search for all paths that contain traces with `cleanse` as part of the name, type:
  `trace:cleanse`

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

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

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

  ```
  category:!SQL Injection
  ```

Performing Simple Searches

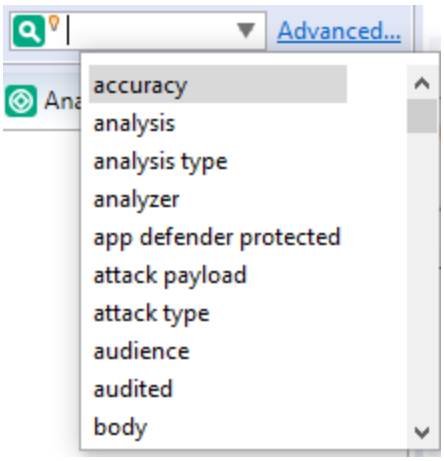
To use the search box to perform a simple search, do one of the following:

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

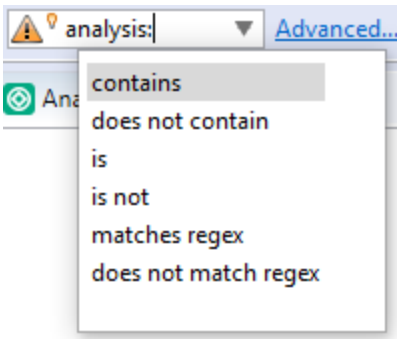
- To select a search term you used previously, click the arrow in the search box, and then select a search term from the list.

To get assistance to compose the comparison for your search string, do the following:

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



2. From the displayed list, double-click an issue attribute to begin your search string.
3. To get 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 the comparison to add to your search string.
5. Type the rest of the search term.

The **Static Analysis Results** view lists all the issues that match your search string.

The plugin saves all the search terms you type for the current session. To select a search term you used previously, click the arrow in the search box, and then select a search term. (After you close Eclipse, the saved search terms are discarded.)

To create complex search strings can involve several steps. If you type an invalid search string, the magnifying glass icon in the text field changes to a warning icon to notify you of the error. Click the warning sign to view information about the search term error.

The advanced search feature makes it easier to build complex search strings. For a description of this feature and instructions on how to use it, see "Performing Advanced Searches" below.

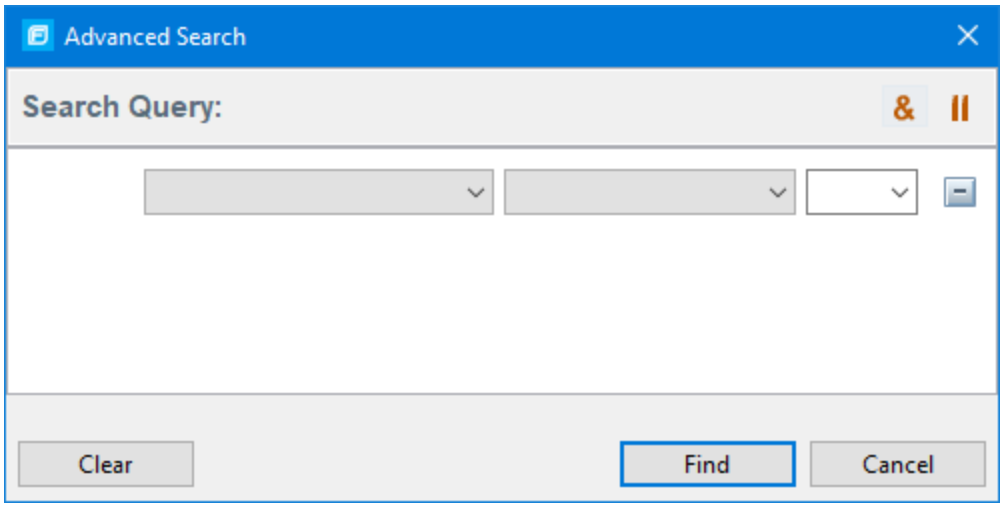
Performing Advanced Searches

You can use the advanced search feature to build complex search strings.

Note: The advanced search feature is not available in the Eclipse Remediation Plugin.

To use the advanced search feature:

1. To the right of the search box, click **Advanced**.



2. To create your search query:
   a. From the list of the left, select the modifier.
   b. From the middle list, select the comparison and type.
   c. From the list on the right, select the search term.

   The list for the search term includes the known values in the current scan for the specified attribute. However, you can type any value into this field. To specify an unqualified search term, select **Any Attribute** from the bottom of the modifier list.
3. To add another query row, do one of the following:

- To add an AND query row, in the top right corner of the dialog box, click **AND** (&).
- To add an OR query row, in the top right corner of the dialog box, click **OR**(||).

4. Add as many query rows as you need for the search.
5. To delete a row, to the right of the row, click **Delete** . To remove all rows, click **Clear**.
6. Click **Find**.

Note: As you build your search string, the Advanced Search dialog box displays any errors in the status below the search string builder. The **Find** button is only enabled after you resolve all errors.

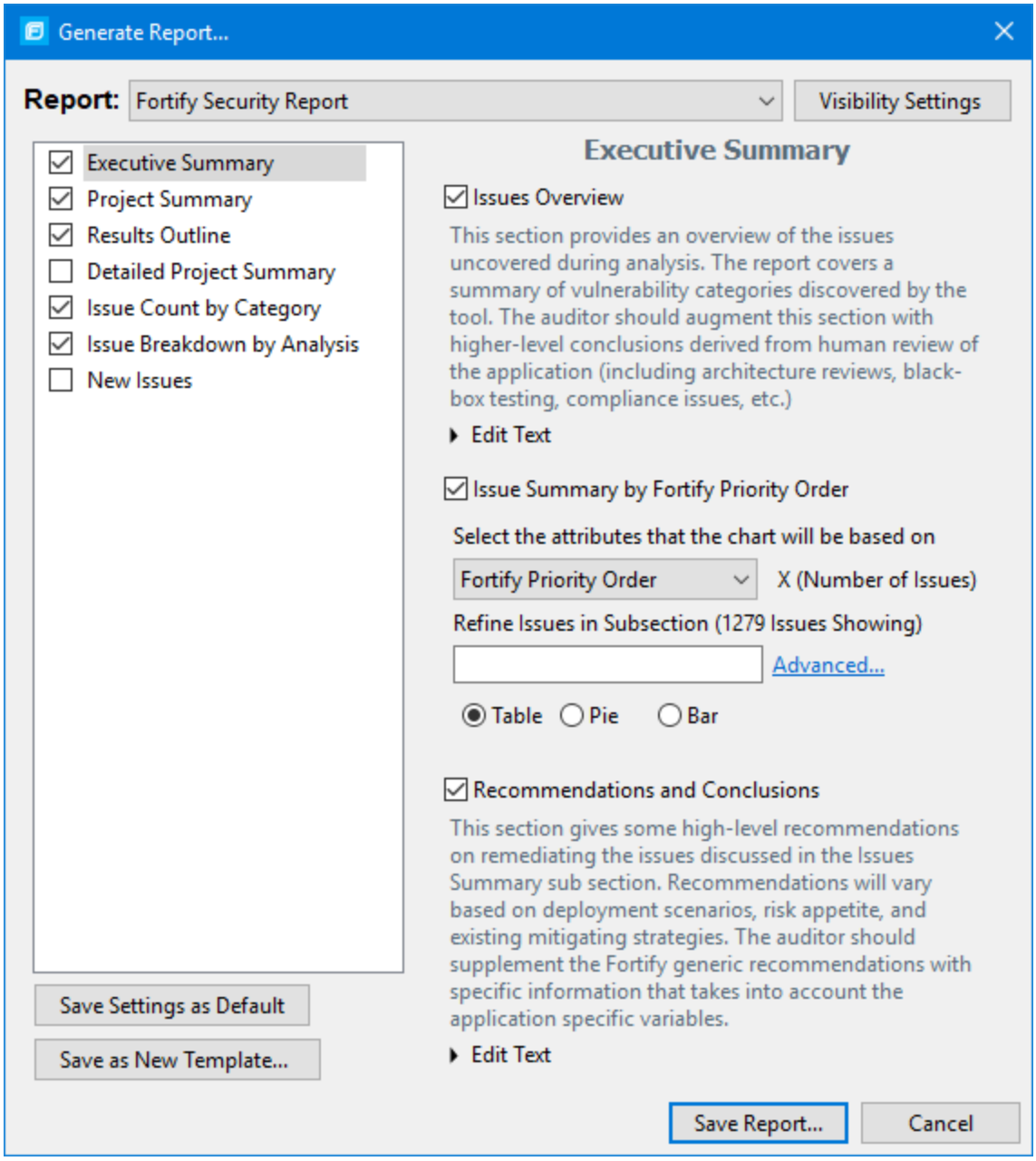
Eclipse Complete Plugin Reports

The Eclipse Complete Plugin provides a flexible reporting infrastructure based on user-configurable report templates. Report templates provide several optional sections and subsections that gather and present specific types of data. The following sections provide information about the default reports and report templates, instructions on how to modify existing reports, and how to create your own reports.

Opening Legacy Report Templates

To open a report template:

1. Select **Fortify > Generate Legacy Report**.
   The Generate Report dialog box opens.



2. Select a report template from the **Report** list.

The Generate Report dialog box displays the report template settings.

Generating Legacy Reports

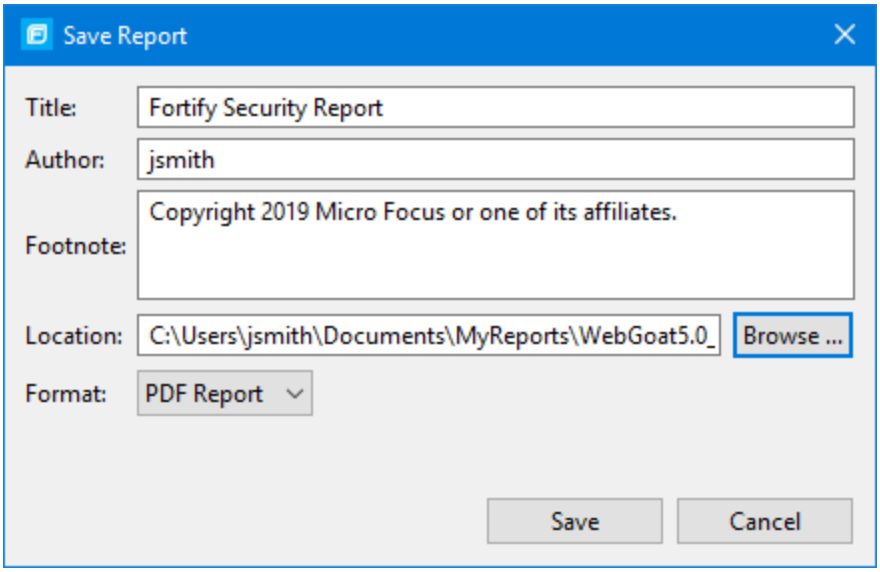
After you select a report template and specify report settings, you generate the report to view the results. You can save report results as PDF, RTF, and XML files.

To run a report:

1. Select **Fortify > Generate Legacy Report**.
2. Select a report template from the **Report** list.

3. (Optional) Make changes to the report section settings.
4. Click **Save Report**.

   The Save Report dialog box opens.



5. Make any necessary changes to the report details, including its location and format.

   Note: If you save the report in rich text format (RTF), you can open the report in an associated application based on the setting of the `com.fortify.model.report.targetEnv` property in the `fortify.properties` configuration file. See the *Micro Focus Fortify Static Code Analyzer Tools Properties Reference Guide* for more information.

6. Click **Save**.

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

Legacy Report Templates

This section describes how to select and edit a legacy report template. If you or another user have edited or created other default report templates, you might not see the default report templates described in this section.

The legacy report templates include:

- **Fortify Developer Workbook**—A comprehensive list of all categories of issues found and multiple examples of each issue. This report also gives a high-level summary of the number of issues in each category.
- **Fortify Scan Summary**—High-level information based on the category of issues that Micro Focus Fortify Static Code Analyzer found as well as a project summary and a detailed project summary.
- **Fortify Security Report**—A mid-level report that provides comprehensive information on the analysis performed and the high-level details of the audit that was performed. It also provides a high-level description and examples of categories that are of the highest priority.

- **OWASP Top Ten *<year>***—High-level summaries of uncovered vulnerabilities organized based on the top ten issues that the Open Web Security Project (OWASP) has identified.

You can modify legacy report templates from the Generate Legacy Report dialog box, or you can edit report templates directly in XML (see "Report Template XML Files" on page 80). The following sections provide information about how to view report templates and customize them to address your reporting needs.

Selecting Report Sections

You can choose sections to include in the report, and you can edit the content displayed in each section.

To select sections to include in the report:

1. Select each section title check box in the list on the left side.
2. Click a section title to view the contents of the section.

The section details are displayed to the right of the dialog box. For instructions on how to edit each section, see "Saving Legacy Report Templates" on page 79.

To remove a section from the report, clear the check box next to the section title.

Editing Report Subsections

When you select a section title, you can edit the contents that display in the report. You can edit text, add or change text variables, or customize the issues shown in a chart or results list.

Editing Text Subsections

To edit a text subsection:

Select the check box next to the subsection title to include this text in the report. A description of the text displays below the subsection title.

1. Click **Edit Text**.

   The text box displays the text and variables to include in the report.
2. Edit the text and text variables.
3. When you edit text subsections, you can insert variables that are defined when you run the report. The following table lists the report variables.

Variable	Description
`$AUDIT_GUIDE_SUMMARY$`	List of filters created with answers to Audit Guide Wizard questions
`$CLASSPATH_LISTING$`	JAR files used in the scan, one relative path per line
`$COMMANDLINE_ARGS$`	Complete list of command-line options (same format as project summary)

Variable	Description
$FILE_LISTING$	List of files scanned, each file in format *<relative file path>* # Lines # kb *<timestamp>*
$FILTERSET_DETAILS$	List of filters the current filter set uses
$FILTERSET_NAME$	Name of the current filter set
$FORTIFY_SCA_VERSION$	Micro Focus Fortify Static Code Analyzer version
$LIBDIR_LISTING$	Libdirs specified for the scan, one relative path per line
$TLOC$	Total lines of code
$NUMBER_OF_FILES$	Total number of files scanned
$PROJECT_BUILD_LABEL$	Build label of project
$PROJECT_NAME$	Build ID
$PROPERTIES$	Complete list of properties set for the analysis phase (same format as project summary)
$RESULTS_CERTIFICATION$	Complete certification detail with a list of validity on a per file basis (same format as project summary)
$RESULTS_CERTIFICATION_SUMMARY$	Short description of certification (same format as project summary)
$RULEPACKS$	Complete list of Rulepacks used for the analysis (same format as project summary)
$SCAN_COMPUTER_ID$	Hostname of machine on which the scan was performed
$SCAN_DATE$	Date of analysis with the default format style for the locale
$SCAN_SUMMARY$	Summary of codebase scanned in format # files, # lines of code
$SCAN_TIME$	Time of analysis phase
$SCAN_USER$	Username for the user who performed the scan

Variable	Description
$SOURCE_BASE_PATH$	Source base path of codebase
$TOTAL_FINDINGS$	Number of findings, not including suppressed or removed issues
$WARNINGS$	Complete list of warnings that occurred
$WARNING_SUMMARY$	Number of warnings found in scan

Editing Results List Subsections

To edit a result list subsection:

1. Select the check box next to the subsection title to include this text in the report.
   A description of the results list displays below the subsection title.
2. Click the issues list heading to expand the options.
3. Select the attributes used to group the results list.
   For the list of attributes to group by, see "Working with Issues" on page 49. If you group by category, the recommendations, abstract, and explanation for the category are also included in the report.
4. (Optional) To refine the issues shown in this subsection with the search function, click **Advanced**.
   For more details about the search syntax, see "Searching for Issues" on page 64.
5. Select or clear the **Limit number of Issues in each group** check box.
6. If you selected the check box, type the number of issues to display per group.

Editing Charts Subsections

To edit a chart subsection:

1. Select the check box next to the subsection title to include this text in the report.
   A chart description is displayed below the subsection title.
2. Select the attributes used to group the chart data.
   For the list of attributes to group by, see "Working with Issues" on page 49.
3. (Optional) To refine the issues shown in this subsection with the search function, click **Advanced**.
   For more details about the search syntax, see "Searching for Issues" on page 64.
4. Select the chart format (table, pie, or bar).

Saving Legacy Report Templates

You can save the current report settings as a new template that you can select later to run more reports.

To save settings as a report template:

1. Select **Fortify > Generate Legacy Report**.
   The Generate Report dialog box opens.
2. Select the report template from the **Report** list.
3. Make changes to the report section and subsection settings.
4. Click **Save as New Template**.

The new report template is saved. When you select the report template name from the **Report** list, the report settings are displayed in the Generate Report dialog box.

Saving Changes to Report Templates

You can save changes to a report template so that your new settings are displayed as the defaults for that template.

To save changes a report template:

1. Select **Fortify > Generate Legacy Report**.
   The Generate Report dialog box opens.
2. Select the report template to save as the default report template from the **Report** list.
3. (Optional) Make changes to the report section and subsection settings.
4. Click **Save Settings as Default**.

Report Template XML Files

Report templates are saved as XML files. You can edit the XML files to make changes or to create new report template files. When you edit the XML files, you can choose the sections and the contents of each section to include in the report template.

The default location for report template XML files is:

`<eclipse_install_dir>/plugins/com.fortify.dev.ide.eclipse_<version>/Core/config/reports`

To customize the logos used in the reports, you can replace `header.jpg` and `footer.jpg` in this directory.

Adding Report Sections

You can add report sections by editing the XML files. In the structure of the XML, the `ReportSection` tag defines a new section. It includes a `Title` tag for the section name, and it must include at least one `Subsection` tag to define the contents of the section in the report. The following XML is the `Results Outline` section of the Fortify Security Report:

```
<ReportSection enabled="false" optionalSubsections="true">
  <Title>Results Outline</Title>
  <SubSection enabled="true">
```

```
    <Title>Overall number of results</Title>
    <Description>Results count</Description>
    <Text>The scan found $TOTAL_FINDINGS$ issues.</Text>
  </SubSection>
  <SubSection enabled="true">
    <Title>Vulnerability Examples by Category</Title>
    <Description>Results summary of the highest severity issues.
     Vulnerability examples are provided by category.</Description>
    <IssueListing limit="1" listing="true">
      <Refinement>severity:(3.0,5.0] confidence:[4.0,5.0]</Refinement>
      <Chart chartType="list">
        <Axis>Category</Axis>
      </Chart>
    </IssueListing>
  </SubSection>
</ReportSection>
```

In the previous example, the `Results Outline` section contains two subsections. The first subsection is a text subsection named `Overall number of results`. The section subsection is a results list named `Vulnerability Examples by Category`. A section can contain any combination of subsections as its contents.

Adding Text Subsections

In a text subsection, you can include the `Title` tag, the `Description` tag, and the `Text` tag. In the `Text` tag, you can provide the default content, although you can edit the content before you generate a report. For a description of the text variables available to use in text subsections, see "Editing Report Subsections" on page 77. The following XML is the `Overall number of results` subsection in the `Results Outline` section:

```
<SubSection enabled="true">
  <Title>Overall number of results</Title>
  <Description>Results count</Description>
  <Text>The scan found $TOTAL_FINDINGS$ issues.</Text>
</SubSection>
```

In this example, the text subsection is titled `Overall number of results`. The description text to describe the purpose of the text is `Results count`. The text in the text field that the user can edit before running a report uses one variable named `$TOTAL_FINDINGS$`.

Adding Results List Subsections

In a results list subsection, you can include the `Title` tag, the `Description` tag, and the `IssueListing` tag. In the `IssueListing` tag, you can define the default content for the limit and set `listing` to `true`. You can include the `Refinement` tag either with or without a default statement,

although you can edit the content before you generate a report. To generate a results list, the `Chart` tag attribute `chartType` is set to `list`. You can also define the `Axis` tag. The following XML is the `Vulnerabilities Examples by Category` subsection in the `Results Outline` section:

```
<SubSection enabled="true">
  <Title>Vulnerability Examples by Category</Title>
  <Description>Results summary of the highest severity issues.
   Vulnerability examples are provided by category.
  </Description>
  <IssueListing limit="1" listing="true">
    <Refinement>severity:(3.0,5.0] confidence:[4.0,5.0]</Refinement>
    <Chart chartType="list">
      <Axis>Category</Axis>
    </Chart>
  </IssueListing>
</SubSection>
```

In this example, the results list subsection is titled `Vulnerability Examples by Category`. The description text to describe the purpose of the subsection is `Results summary of the highest severity issues. Vulnerability examples are provided by category`. This subsection lists (`listing=true`) one issue (`limit="1"`) per Category (the `Axis` tag value) where there are issues that match the statement `severity:(3.0,5.0] confidence:[4.0,5.0]` (the value of the `Refinement` tag).

Adding Charts Subsections

In a chart subsection, you can include the `Title` tag, the `Description` tag, and the `IssueListing` tag. In the `IssueListing` tag, you can define the default content for the limit and set `listing` to `false`. You can include the `Refinement` tag either with or without a default statement, although you can edit the content before generating a report. To generate a pie chart, the `Chart` tag attribute `chartType` is set to `pie`. The options are `table`, `pie`, and `bar`. You can change this setting before you generate the report. You can also define the `Axis` tag.

The following code shows an example of a chart's subsection:

```
<SubSection enabled="true">
  <Title>New Issues</Title>
  <Description>A list of issues discovered since the previous
   analysis</Description>
  <Text>The following issues have been discovered since the
   last scan:</Text>
  <IssueListing limit="-1" listing="false">
    <Refinement />
    <Chart chartType="pie">
      <Axis>New Issue</Axis>
    </Chart>
  </IssueListing>
</SubSection>
```

In this subsection, a chart (`limit="-1" listing="false"`) has the title `New Issues` and a text section that contains the text `The following issues have been discovered since the last scan`. This chart includes all issues (the `Refinement` tag is empty) and groups the issues on the value of `New Issues` (the value of the `Axis` tag). This chart is displayed as a pie chart (`chartType="pie"`).

Configuring a Connection to Fortify Software Security Center

To configure a connection to Micro Focus Fortify Software Security Center, you need the following:

- The URL for your Fortify Software Security Center and if necessary, the proxy server and port number for the connection
- If you will connect to Fortify Software Security Center using X.509 SSO, download and deploy the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files to the Java JRE used for Eclipse.

To configure a connection to Fortify Software Security Center:

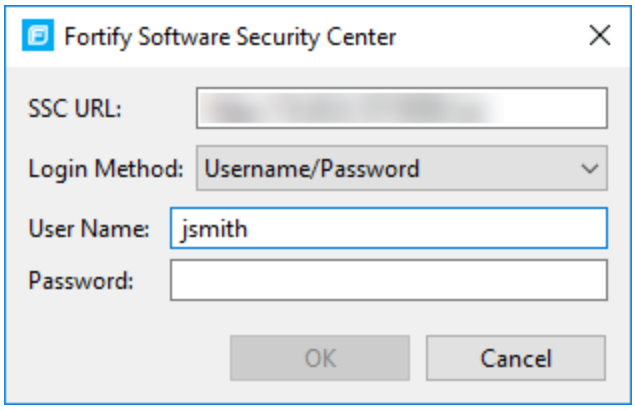
1. Select **Fortify > Options**.
2. In the left panel, select **Server Configuration**.
3. Under **Software Security Center Configuration**, specify the **Server URL** for your Fortify Software Security Center (for example, `http://111.0.0.1:8180/ssc`).
4. If required, specify the proxy server and port number.
5. Click **Apply**, and then click **OK**.

Logging in to Fortify Software Security Center

The first time you perform an operation that requires a connection to Micro Focus Fortify Software Security Center such as uploading an audit project or opening a collaborative application, you are prompted to log in.

To log in to Fortify Software Security Center:

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



2. 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.
X.509 SSO	a. Click the **Browse** button to the right of **Certificate**. b. In the Browser for Certificate dialog box, locate the p12 package with the certificate, and then click **Open**. c. Type the password if required.
Kerberos SSO	No additional information is required.

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

Synchronizing with Fortify Software Security Center

You can automatically upload your changes to an application version on Micro Focus Fortify Software Security Center each time you load, merge, save, or scan your local project. This automatic synchronization helps facilitate collaborative auditing, and enables you to synchronize any offline changes each time you connect to the server.

Note: Automatic synchronization requires that you specify an application version that already exists in Fortify Software Security Center. If the application version does not exist in Fortify

Software Security Center, you must first create it. For instructions, see the *Micro Focus Fortify Software Security Center User Guide*.

To enable or disable synchronization to the server:

1. Select **Fortify > Options**.
2. Click **Default Project Settings** in the left panel.
3. Select the **Synchronize Options** tab.
4. To enable synchronization to the server, select **Synchronize project with server**.

Scheduling Synchronization

You can customize which action synchronizes your local version of the project with the server. For example, you can specify that synchronization only occurs when you merge or scan a project.

To customize when synchronization occurs:

1. Right-click a project.
2. Select **Properties**.
3. Select **Fortify Project Properties**.
4. You can schedule synchronization for either the current project or the workspace:
   - To schedule synchronization for only the current project, select **Enable project specific settings**.
   - To schedule synchronization for the workspace, click **Configure Workspace Settings**.
5. Select the **Synchronize Options** tab.
6. Select the options that you want to exclude from automatic synchronization.
7. Click **OK**.

Refreshing Permissions From Fortify Software Security Center

The Micro Focus Fortify Software Security Center administrator assigns roles to users that determine the actions they can perform in Fortify Software Security Center. When you work on a collaborative audit and the administrator changes your auditing permissions, you might need to refresh the permissions in the Eclipse Complete Plugin.

To refresh your permissions from Fortify Software Security Center:

1. Select **Fortify > Options**.
2. In the left panel, select **Server Configuration**.
3. Click **Refresh Permissions for the Current Audit**.
4. Click **OK**.

Working with Audit Projects

After you scan a project, you can audit the analysis results. You can also audit the results of a collaborative audit from Micro Focus Fortify Software Security Center.

Opening an Audit Project

To open an audit project:

1. Select **Fortify > Open Audit Project**.
   The Select Audit Project dialog box opens.
2. Browse to and select the FPR file, and then click **Open**.

Opening an Existing Audit

You can open a local, previously saved audit, and continue your work. Alternatively, you can open an audit that someone else performed on a different machine.

To open a locally previously-saved audit:

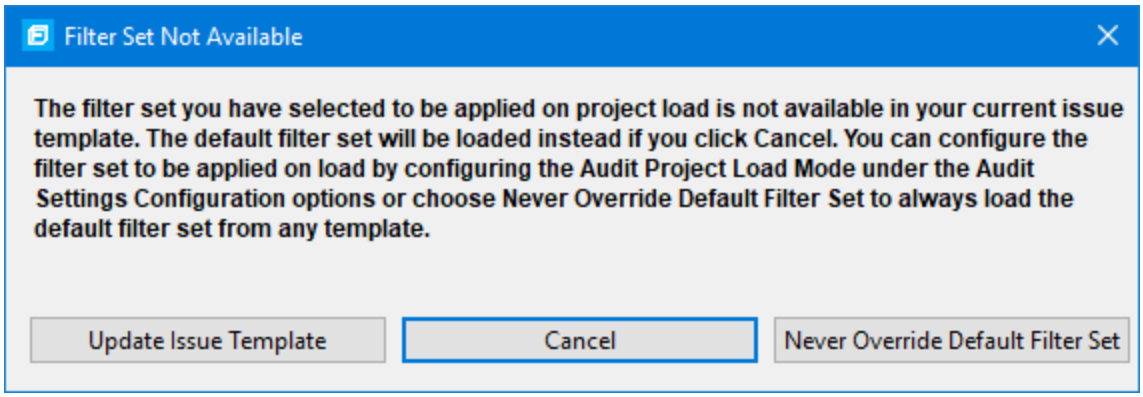
1. From Eclipse, select a project.
2. Select **Fortify > Load Saved Audit Project**.

To open an externally generated audit:

- Select **Fortify > Open Audit Project**.

Opening Audit Projects Without the Default Filter Set

If you open an audit project that does not contain the filter set specified as the default filter set for new projects (by default, this is the Quick View filter set), a message is displayed to inform you that the filter set is not available in the audit project's issue template.



The default filter set from the template is loaded at startup, regardless of the setting. This would also happen, for example, with any FPR files downloaded from the Fortify on Demand Server.

To resolve this, do one of the following:

- To apply the default filter set from the current issue template, click **Cancel**.
- To update the issue template for the project, click **Update Issue Template**.

  After you select **Update Issue Template**, some of the filter sets that were available before the update, for example Developer View and Critical Exposure, are no longer available.

  A warning is displayed to let you know that you cannot undo the update.
- To ensure that the default filter set for the project is never overridden, click **Never Override Default Filter Set**.

Exporting an Audit Project

To save an audit project in a specific location:

1. Select **Fortify > Export Audit Project**.
2. Browse to where you want to save the FPR.
3. Type a file name, and then click **Save**.

Obtaining New Results

This section covers how to obtain new results for an existing audit.

To obtain results for an existing audit:

1. From Eclipse, open the Java or C/C++ perspective.
2. In the **Package Explorer** view, right-click the project, and then select **Analyze Project** from the shortcut menu.

Merging Audit Data

Audit data includes the custom tags and comments that were added to an issue. You can merge the audit data for your project with audit data from another results file. Comments are merged into a chronological list and custom tag values are updated. If custom tag values conflict (if the same tag is set to different values for a given issue), the Eclipse Complete Plugin prompts you to resolve the conflict.

Note: Issues are not merged. Merged results include only the issues found in the latest scan. Issues uncovered in the older scan that were not uncovered in the latest scan are marked as Removed and are hidden by default.

Make sure that the projects you merge contain the same analysis information. That is, make sure that the scans were performed on the same source code (no missing libraries or files), the Micro Focus Fortify Static Code Analyzer settings were the same, and the scan was performed using the same security content.

To merge projects:

1. Open a project in the Eclipse Complete Plugin.
2. Select **Fortify > Merge Audit Projects**.
3. Select an audit project (FPR file), and then click **Open**.

   The Progress Information dialog box opens. When complete, the Merge dialog box opens.
4. Click **Yes** to confirm the number of issues added or removed from the file.

   Note: If the scan is identical, no issues are added or removed.

The project now contains all audit data from both result files.

Performing a Collaborative Audit

You can audit a project on Micro Focus Fortify Software Security Center collaboratively with other Fortify Software Security Center users. Before you can access audit results from Fortify Software Security Center, you must have configured a connection to Fortify Software Security Center. See "Configuring a Connection to Fortify Software Security Center" on page 83.

To start a collaborative audit:

1. Select **Fortify > Open Collaborative Audit**.

   If you already have an audit project open, close it.
2. If prompted, provide your Fortify Software Security Center credentials.
3. In the Choose Application and Version Mapping for Collaboration dialog box, select an application version, and then click **OK**.

   The audit project is downloaded from Fortify Software Security Center and opened in the Fortify Audit perspective.
4. Audit the project as described in "About Viewing Scan Results" on page 30.
5. When you have completed the audit, select **Fortify > Upload Audit Project**.
6. Click **OK**.

Note: If necessary, you can refresh your Fortify Software Security Center audit permission settings. See "Refreshing Permissions From Fortify Software Security Center" on page 85.

Uploading Audit Results to Fortify Software Security Center

Before you can upload audit results (audit project) to Fortify Software Security Center, you must have configured a connection to Fortify Software Security Center. See "Configuring a Connection to Fortify Software Security Center" on page 83.

When you work on a collaborative audit and the project was downloaded from Micro Focus Fortify Software Security Center, the Eclipse Complete Plugin retains the application version for the audit project. If you want to upload the audit project to a different application version, you need to disconnect the audit project from Fortify Software Security Center before you upload the results. To disconnect the current audit project from Fortify Software Security Center, select **Fortify > Options**, click **Server Configuration**, and then click **Disconnect the Current Audit**.

Note: If you created any custom tags or filter sets for your project's issue template, you must first commit them to Fortify Software Security Center before you upload the project so that information is also uploaded. See "Committing Custom Tags to Fortify Software Security Center" on page 101 and "Committing Filter Sets and Folders" on page 93 for more information.

Note: By default, Micro Focus Fortify Software Security Center ignores uploaded scans performed in quick scan mode. However, you can configure your Fortify Software Security Center application version so that uploaded audit projects scanned in quick scan mode are processed. For more information, see analysis results processing rules in the *Micro Focus Fortify Software Security Center User Guide*.

To upload results to Fortify Software Security Center:

1. Select **Fortify > Upload Audit Project**.
2. If prompted, type your Fortify Software Security Center credentials.
3. If the audit project is not already associated with an application version, select an application version, and then click **OK**.

   Note: If you see a message that the application version is not committed or does not exist, this indicates that you opened an audit project that was previously associated with an application version that does not exist on Fortify Software Security Center to which Fortify Plugins for Eclipse is currently connected. Disconnect the audit project from Fortify Software Security Center as described previously in this section.

   A message notifies you when the upload is complete.
4. Click **OK**.

Updates you made to issues including comments and tag values (for tags that already exist for the application version on Fortify Software Security Center) are uploaded.

About Issue Templates

Micro Focus Fortify Static Code Analyzer produces comprehensive results for source code analysis. On large codebases, these results can be overwhelming. The issue template assigned to your projects enables you to sort and filter the results to best suit your needs. The filtering and sorting mechanisms appropriate during a given phase in the development process can change depending on the phase of development. Similarly, the filtering and sorting mechanisms might vary depending on the role of the user.

You can sort issues by grouping them into folders, which are logically defined sets of issues presented in the tabs on the Static Analysis Results. You can further customize the sorting to provide custom definitions for the folders into which the issues are sorted. You can provide definitions for any number of folders, whose contents are then defined by filters. Filters can either alter the visibility of an issue or place it into a folder. When used to sort issues into folders, you define the nature of the issues that appear in the customized folders.

You group filters into filter sets and then use the filter sets to sort and filter the issues displayed. An issue template can contain definitions for multiple filter sets. Using multiple filter sets in an audit project

enables you to quickly change the sorting and visibility of the issues you are auditing. For example, the default issue template used in the interface provides two filter sets. These filter sets provide an increasingly restrictive view of security-related issues. Defining multiple filter sets for an audit project enables different views for different users, and a customized view does not affect any other views.

In addition to providing sorting and filtering mechanisms, you can also customize the auditing process by defining custom tags in the issue template. Auditors associate custom tags with issues during auditing. For example, you can use custom tags to track impact, severity, or priority of an issue using the same names and values used to track these attributes in other systems, such as a bug tracker application.

Issue templates contain the following settings:

- Folder filters—Control how issues are sorted into the folders
- Visibility filters—Control which issues are shown and hidden
- Filter sets—Group folder and/or visibility filters
- Folder properties—Name, color, and the filter set in which it is active
- Custom tags—Specify which audit fields are displayed and the values for each

The issue template applied to an audit project is determined using the following preference order:

1. Template that exists in the audit project
2. Template `<eclipse_install_dir>/plugins/com.fortify.dev.ide.eclipse_<version>/Core/config/filters/defaulttemplate.xml`
3. Template `<eclipse_install_dir>/plugins/com.fortify.dev.ide.eclipse_<version>/Core/config/rules/defaulttemplate.xml`
4. Embedded Fortify default template

Configuring Custom Filter Sets and Filters

If the filter sets available in the Eclipse Complete Plugin do not exactly suit your needs, you can create your own, either by using the filter wizard, or by copying and then modifying an existing filter set.

If you are performing collaborative audits on Micro Focus Fortify Software Security Center, you can synchronize your custom filters with Fortify Software Security Center. For more information, see "Committing Filter Sets and Folders" on page 93 and "Synchronizing Filter Sets and Folders" on page 94.

This section provides instructions on how to:

- Create a new filter set
- Create filters from the **Issues** view and add them to a filter set
- Create filters on the **Filters** tab and add them to a filter set
- Copy a filter to a different filter set

Creating a New Filter Set

To create a new filter set, copy an existing set and modify the settings.

To create a new filter set:

1. Select **Fortify > Project Configuration**.
2. Click the **Filter Sets** tab.
3. Next to **Filter Sets**, click **Add Filter Set**  .
   The Add New Filter Set dialog box opens.
4. Type a name for the new filter set.
5. Select an existing filter set to copy.
6. Click **OK**.

A new filter set with the same folders, visibility filters, and folder filters as the copied filter set is created.

Creating a Filter from the Static Analysis Results View

When a folder list includes an issue that you want to hide or direct to another folder, you can create a new filter using the filter wizard. The wizard displays all the attributes that match the conditions in the filter.

Note: To find the filter that directed the issue to the folder, right-click the issue, and then select **Why is this issue here?** To find the filter that hid an issue, right-click the issue, and then select **Why is this issue hidden?**

To create a new filter from an issue:

1. In the **Static Analysis Results** view, select a filter set from the **Filter Set** list.
2. Right-click an issue, and then select **Create Filter**.
   The Create Filter dialog box lists suggested conditions.
3. To see all the conditions, select the **Show all conditions** check box.
4. Select the conditions you want to use in the filter.
   You can fine tune the filter later by modifying it on the **Filter** tab.
5. Select the type of filter you want to create, as follows:
   - To create a visibility filter, select **Hide Issue**.
   - To create a folder filter, select **Set Folder to**, and then select the folder name or select **Other Folder** to add an existing folder or create a new one.
     A new folder is displayed in this filter set only.
6. Click **Create Filter**.
   The wizard places the new filter at the end of the filter list. For folder filters, this gives the new filter the highest priority. Issues that match the new folder filter appear in the targeted folder.
7. (Optional) For folder filters, drag the filter higher in the folder filter list to change the priority.

The issues are sorted with the new filter.

Note: The filter is created only in the selected filter set.

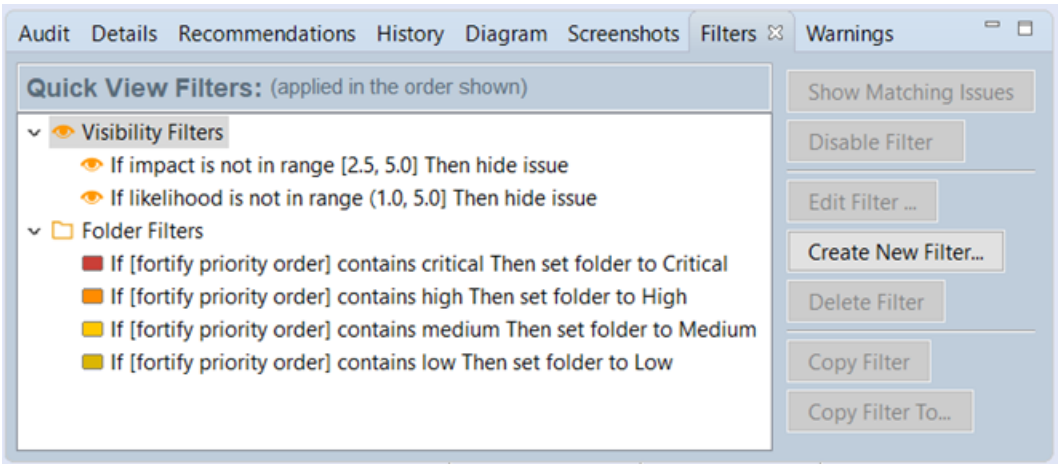
Creating a Filter from the Issue Auditing View

Use the **Filters** tab in the Issue Auditing view to create visibility filters and folder filters.

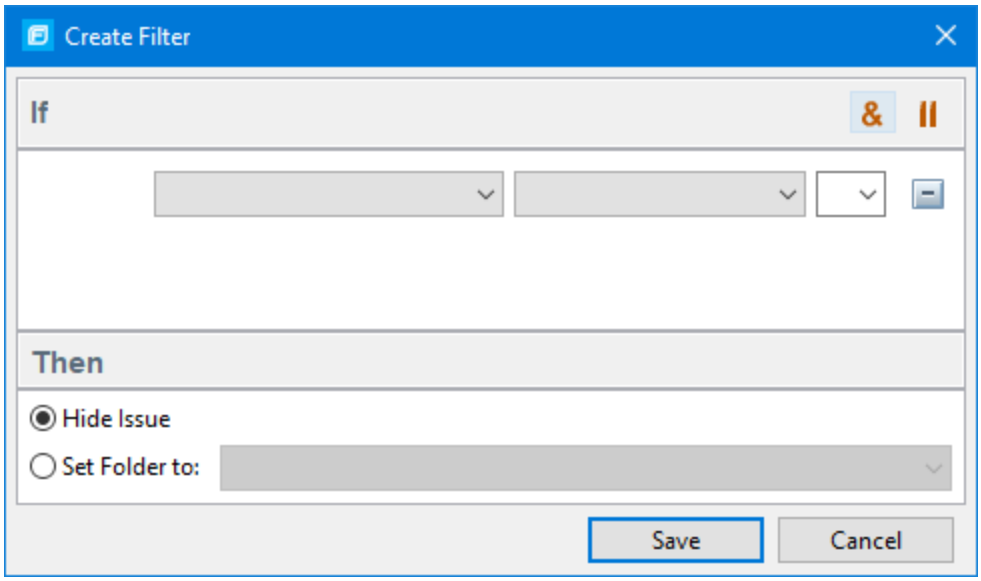
Folder filters are applied in order and the issue is directed to the last folder filter it matches in the list.

To create a new filter on the **Filters** tab:

1. From the **Filter Set** list, select a filter set.
2. Click the **Filters** tab in the Issue Auditing view.



3. Right-click **Visibility Filters** or **Folder Filters**, and then select **Create New Filter**.
   The Create Filter dialog box opens.



4. From the first list, select an issue attribute.
   The second list is automatically populated.
5. From the second list, select how to match the value.

The third list contains the possible values for the attribute.

6. Select a value or specify a range as instructed in the **If** line.
7. Set **Then** to one of the following options:
   - To create a visibility filter, select **Hide Issue**.
   - To create a folder filter, select **Set Folder to**, and then select the folder name or select **Other Folder** to add a folder from another filter set or create a new folder.
8. Click **Save**.

   The new filter is displayed at the end of the list. For folder filters, this gives the new filter the highest priority. Issues that match the new folder filter appear in the targeted folder.
9. (Optional) For folder filters, drag the filter higher in the folder filter list to change the priority.

The issues are sorted with the new filter.

Note: The filter is created in the selected filter set only.

Copying a Filter from One Filter Set to Another

Filter settings are local to a filter set. However, you can copy the filter to another filter set in the audit project. If you copy a folder filter to another set and that folder is not already active in the set, the folder is automatically added.

To copy a filter:

1. In the **Static Analysis Results** view, select a filter set from the **Filter Set** list.
2. Click the **Filters** tab in the Issue Auditing view.
3. Right-click a filter, and then select **Copy Filter To** from the shortcut menu.

   The Select a Filter Set dialog box opens with a list of all the filter sets.
4. Select a filter set, and then click **OK**.

   The filter is added to the filter set in the last position.
5. (Optional) For folder filters, you can adjust the order of the filter list by dragging and dropping the filter to a different location in the list.

Committing Filter Sets and Folders

If you want to upload filter sets and folders to an issue template on Micro Focus Fortify Software Security Center, do the following:

1. Select **Fortify > Project Configuration**.
2. Click the **Filter Sets** tab.
3. Select the filter set from the list.
4. Click **Commit**.
5. If required, provide your Fortify Software Security Center credentials.

   The Update Existing Issue Template or Add Issue Template dialog box opens, depending on whether the issue template already exists in Fortify Software Security Center.

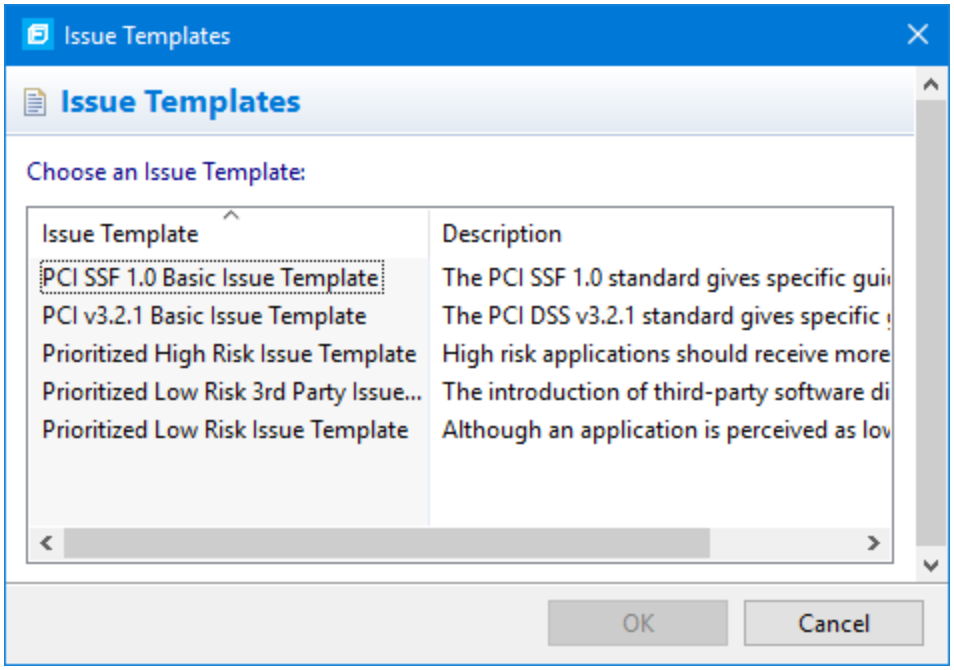
6. Do one of the following:
   a. To upload filter sets and folders to the issue template, click **Yes**.
   b. To add the issue template that contains the current set of custom tags to Fortify Software Security Center, click **Yes**.

Synchronizing Filter Sets and Folders

To download filter sets and folders configured from Micro Focus Fortify Software Security Center:

1. Select **Fortify > Project Configuration**.
2. Click the **Filter Sets** tab.
3. Click **Synchronize**.

   A message advises you that downloading filter sets and folders from Fortify Software Security Center overwrites your local filter sets and folders.
4. To proceed with the synchronization, click **Yes**.
5. If required, provide your Fortify Software Security Center credentials, and then click **OK**.



   If the current issue template does not exist on Fortify Software Security Center, do the following:
   a. In the **Issue Template** column, select an issue template name.
   b. Click **OK**.
6. The Eclipse Complete Plugin downloads the filter sets and folders from the selected issue template on Fortify Software Security Center, and overwrites your current issue template.

Setting the Default Filter Set

To specify the default filter set used to view scan findings:

1. In the **Static Analysis Results** view, click the **Filter Set** list, and then select **Edit**.
   The Project Configuration dialog box opens to the **Filter Sets** tab.
2. In the **Filter Sets** list, select the filter set you want to use as the default for the issue template.
3. Select the **Default filter set** check box, and then click **OK**.

Managing Folders

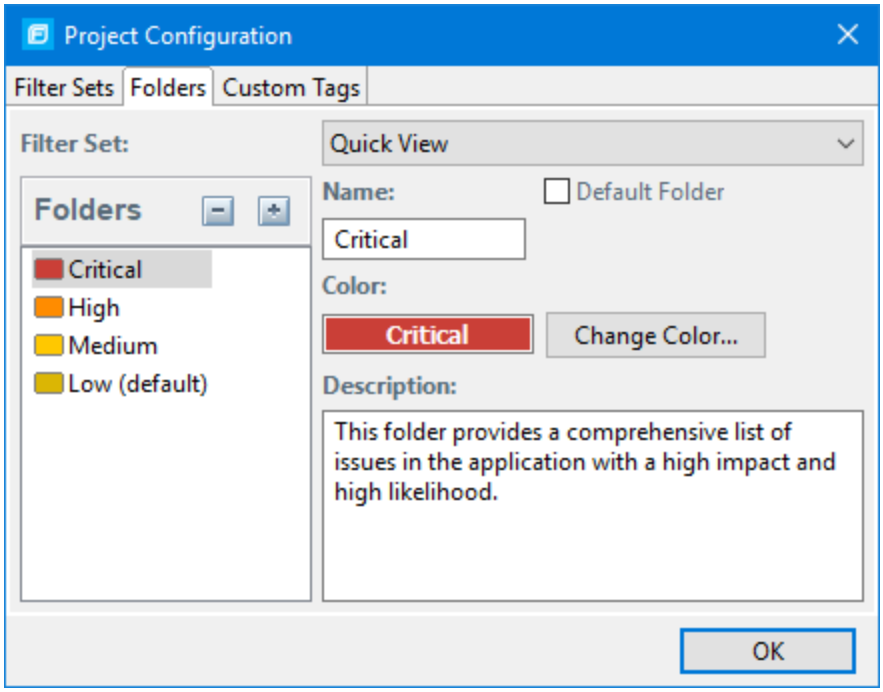
Folders are logical sets of issues that are defined by the filters in the active filter set. Even though a folder can appear in more than one filter set, the contents might differ depending on the filters in that filter set that target the folder. To accommodate filter sets that provide sorting mechanisms with little overlap, you can have filter sets with different folders. Folders are defined independent of the filter sets they may appear in. For example, a filter set might place low priority issues into a red folder that is labeled "Hot."

Creating a Folder

You can create a new folder so that you can display a group of issues you have filtered to the folder. Folders must have unique names.

To create a new folder:

1. Select **Fortify > Project Configuration**.
2. Click the **Folders** tab.
   The **Folders** panel on the left lists the folders for the filter set selected in the **Folder for Filter Set** list. Fields on the right show the name, color, and description of the selected folder.



3. To associate the folder with an existing filter set, select the filter set from the **Filter Set** list.

   Select **(All Folders)** to create a new folder in the issue template without associating the folder to a specific filter set. You can associate the folder with an existing filter set later.

   Note: Selecting a filter set updates the **Folders** list to display the folders that are associated with the selected filter set.

4. To add a folder:

   a. Next to **Folders**, click **Add Folder**  .

   The Add Folder dialog box opens.

   Note: If you have created folders in other filter sets, the Add New Folder to Filter Set dialog box opens. Click **Create New**.

   b. Type a unique name for the new folder, and then select a folder color.

   c. Click **OK**.

   The folder is added to the bottom of the folder list.

5. In the **Description** box, type a description for the new folder.
6. To change the tab position of the folder on the **Static Analysis Results** view, drag the folder up or down in the **Folders** list.

   The top position is on the left and the bottom position is on the right.

7. To put all issues that do not match a folder filter into this folder, select the **Default Folder** check box.
8. Click **OK**.

The folder is displayed as a tab with the other folders. If you selected default, all issues that do not match a folder filter are displayed. The new folder is added to the issue template for the audit project.

Note: To display issues in this folder, create a folder filter that targets the new folder. For more information, see "Creating a Filter from the Static Analysis Results View" on page 91 and "Creating a Filter from the Issue Auditing View" on page 92.

Adding a Folder to a Filter Set

This section describes how to enable an existing folder in a filter set. Create a new folder that appears only in the selected filter set using the instructions in "Creating a Folder" on the previous page. To display issues in this folder, create a folder filter that targets the new folder.

To add a folder to a filter set:

1. Select **Fortify > Project Configuration**.

   The Project Configuration dialog box opens.

2. Click the **Folders** tab.
3. Click the **Filter Set** list to select the filter set to which you want to add a folder.

   The **Folders** list displays the folders in the selected filter set.

4. Next to **Folders**, click **Add Folder**  .
   The Add New Folder to Filter Set dialog box opens.

   Note: If the selected filter set already includes all existing folders, the Create Folder dialog box opens and you can create a new folder for the selected filter set.
5. Select the folder to add to the selected filter set, and then click **Select**.
6. Click **OK**.

The folder is displayed as a tab along with the other folders.

Renaming a Folder

You can rename a folder. Modifying the name of a folder is a global change reflected in all filter sets.

To rename a folder:

1. Select **Fortify > Project Configuration**.
2. Click the **Folders** tab.
3. In the **Filter Set** list, select **(All Folders)**.
4. Select the folder in the **Folders** list.
   The folder properties are displayed on the right.
5. Type the new name for the folder.
   The folder name changes in the **Folders** list as you type.
6. Click **OK**.

The new folder name displays on the tabs.

Removing a Folder

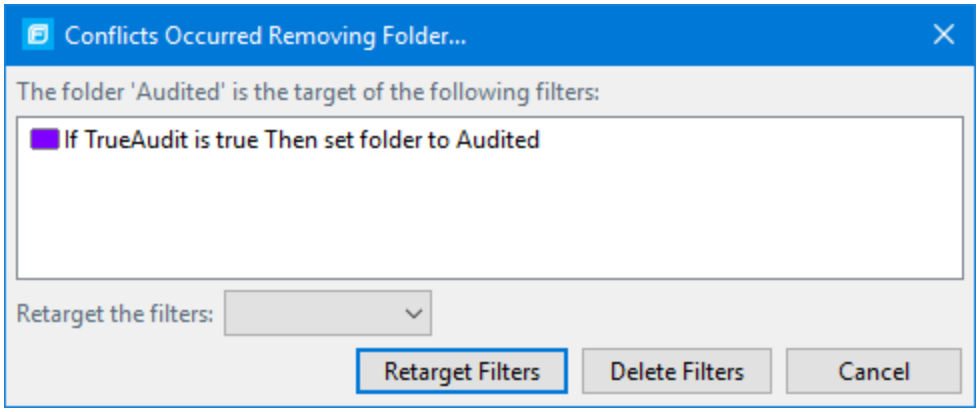
You can remove a folder from a filter set without removing it from other filter sets.

To remove a folder:

1. Select **Fortify > Project Configuration**.
2. Click the **Folders** tab.
3. Select a filter set from the **Filter Set** list.
   The **Folders** list displays the folders in the selected filter set.
4. Select the folder, and then next to **Folders**, click **Delete Folder** .

   Note: The folder is removed only from the selected filter set.

If the folder is a target of a folder filter, the Conflicts Occurred Removing Folder dialog box opens.



Do one of the following:

a. To target the filter to a different folder, select a folder from the **Retarget the filters** list, and then click **Retarget Filters**.
b. To delete the filter, click **Delete Filters**, and then click **Yes** to confirm the deletion.

5. Click **OK** to close the Project Configuration dialog box.

The folder is no longer displayed as a tab in the **Static Analysis Results** view.

Configuring Custom Tags for Auditing

To audit code in Micro Focus Fortify Software Security Center, the security team examines project scan results (FPR) and assigns values to custom tags associated with application version issues. The development team can then use these tag values to determine which issues to address and in what order.

The Analysis tag is provided by default. The **Analysis** tag is a list-type tag and has the following valid values: Not an Issue, Reliability Issue, Bad Practice, Suspicious, and Exploitable. You can modify the **Analysis** tag attributes, change the tag values, or add new values based on your auditing needs.

To refine your auditing process, you can define your own custom tags. You can create the following types of custom tags: list, decimal, string, and date. For example, you could create a list-type custom tag to track the sign-off process for an issue. After a developer audits his own issues, a security expert can review those same issues and mark each as “approved” or “not approved.”

You can add the following attributes to your custom tags:

- Extensible—This enables users to create a new value while auditing, even without the permission to manage custom tags.
- Restricted—This restricts who can set the tag value on an issue. Administrators, security leads, and managers have permission to audit restricted tags.

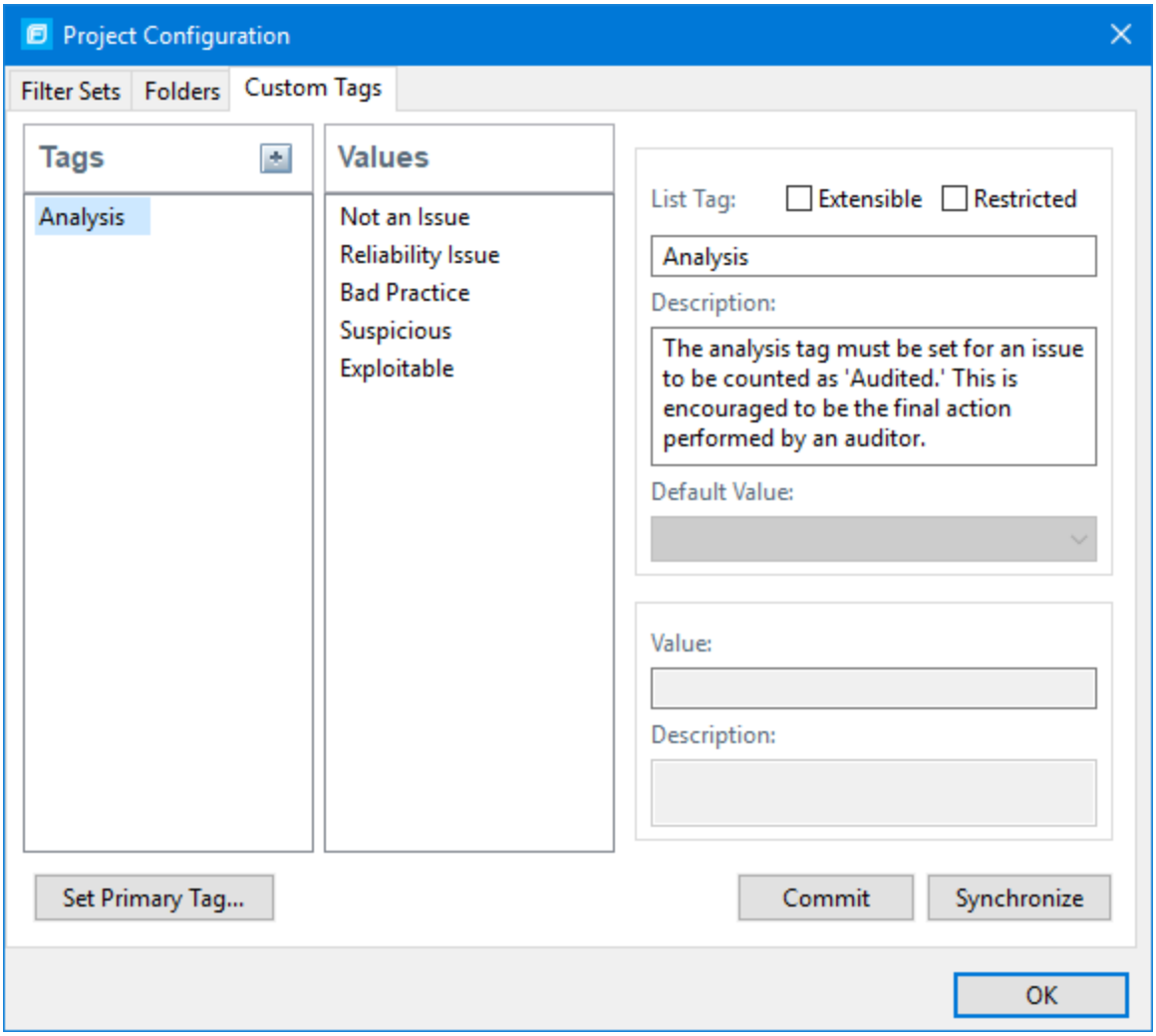
After you define a custom tag, it is displayed below the **Analysis** tag, which enables you to specify values as they relate to specific issues. Custom tags are also available in other areas of the interface, such as in the **Group By** list to group issues in a folder, in the search field as a search modifier (similarly available as a modifier for filters), and in the project summary graph as an attribute by which to graphically sort issues.

Adding a Custom Tag

You can create custom tags to use in auditing results. Custom tags are project-wide and are saved as part of an issue template.

To add a custom tag:

1. Select **Fortify > Project Configuration**.
2. Select the **Custom Tags** tab.



3. Next to **Tags**, click **Add Tag**.

   Note: If you previously hid tags, these are listed and you can re-enable them. To create a new tag, click **Create New**.

   The Add New Tag dialog box opens.
4. In the **Name** box, type a name for the new tag.
5. From the **Type** list, select one of the following tag types:

- **List**—Accepts selection from a list of values that you specify for the tag
- **Date**—Accepts a calendar date
- **Decimal**—Accepts a number with a precision of up to 18 (up to 9 decimal places)
- **Text**—Accepts a string with up to 500 characters (HTML/XML tags and newlines are not allowed)

6. Click **OK**.

   The **Tags** list now includes the new tag.
7. Configure any or all the following optional tag settings:
   - To allow users to add new values for a list-type tag in an audit, leave the **Extensible** check box selected.
   - To allow only administrators, security leads, and managers to set this tag on an issue, select the **Restricted** check box.
   - Type a description of the custom tag in the **Description** box.
   - For a list-type tag, from the **Default Value** list, select the default value for the tag.

     If you do not specify a default value, the default is null.
8. To add a value for a list-type tag, do the following:
   a. From the **Tags** list, select the tag name.
   b. Next to **Values**, click **Add Value**  .
   c. In the Enter Value dialog box, type a value, and then click **OK**.
   d. Type a description of the value in the **Description** box.
   e. Repeat steps a through d for each additional value required for the new tag.
9. To make this custom tag the primary tag:

   Note: You can only set a list-type tag as a primary tag.

   a. Click **Set Primary Tag**.
   b. Select the custom tag from the **Primary Tag** list, and then click **OK**.

   The primary tag determines the audit status for each issue as well as the audit icon in the **Static Analysis Results** view. By default, the primary tag is **Analysis**.

The **Audit** tab in the Issue Auditing view now displays the new tag and its default value (if you assigned one).

Hiding a Custom Tag

If you hide a custom tag, it is no longer available on the Issue Auditing view's **Audit** tab or as a search or filter option.

To hide a custom tag:

1. Select **Fortify > Project Configuration**.
   The Project Configuration dialog box opens.
2. Click the **Custom Tags** tab.
3. Select the tag from the **Tags** list.
4. Next to **Tags**, click **Hide Tag**  .
   This action hides the tag from your available custom tags. You can make this tag available again when you add a custom tag (see "Adding a Custom Tag" on page 99).
5. Click **OK**.

If you hide a tag that has an associated filter, you are prompted to delete the filter.

Committing Custom Tags to Fortify Software Security Center

To commit custom tags to Micro Focus Fortify Software Security Center:

1. With an audit project open, select **Fortify > Project Configuration**.
2. Select the **Custom Tags** tab.
3. Click **Commit**.

   Note: Any list-type custom tags without values are not uploaded to Fortify Software Security Center.

4. If prompted, type your Fortify Software Security Center credentials.
   The Custom Tag Upload dialog box opens.
5. Do one of the following:
   - If the issue template and the application version already exist on Fortify Software Security Center:
     - To upload the custom tags to the global pool and assign them to the application version, click **Yes**.
     - To upload the custom tags to the global pool without assigning them to the application version, click **No**.
     - To prevent uploading the custom tags to Fortify Software Security Center, click **Cancel**.
   - If the issue template does not exist on Fortify Software Security Center:
     - To upload the custom tags to the global pool only on Fortify Software Security Center, click **Yes**.
     - To prevent uploading the custom tags to Fortify Software Security Center, click **No**.

Synchronizing Custom Tags with Fortify Software Security Center

To synchronize custom tags for an audit project that has been uploaded to Micro Focus Fortify Software Security Center.

1. Select **Fortify > Project Configuration**.
2. Select the **Custom Tags** tab.

3. Select the custom tag.
4. Click **Synchronize**.
5. If required, type your Fortify Software Security Center credentials.

   The Custom Tag Download dialog box opens.
6. If the application version and the issue template both exist on Fortify Software Security Center, select either **Application Version** or **Issue Template** to specify from where to download the custom tags.
7. To download custom tags from the issue template, click **Yes**.

Issue Template Sharing

Once an issue template is associated with an audit project, all changes made to that template, such as the addition of folders, custom tags, filter sets, or filters, apply to the audit project. The issue template is stored in the FPR when the audit project is saved. For information about how to associate the issue template with an audit project, see "Importing an Issue Template" below. With issue templates, you can use the same project settings for another project.

Exporting an Issue Template

Exporting an issue template creates a file that contains the filter sets, folders, and custom tags for the current project. After you export an issue template, you can import it into another audit project file.

To export an issue template:

1. Select **Fortify > Project Configuration**.
2. Click the **Filter Sets** tab.
3. Click **Export**.

   The Select a Template File Location dialog box opens.
4. Browse to the location where you want to save the file.
5. Type a file name without an extension.
6. Click **Save**.

The current template settings are saved to an XML file.

Importing an Issue Template

Importing an issue template overwrites the audit project configuration settings. The local filter sets and custom tags are replaced with the filter sets and custom tags in the issue template.

To import an issue template:

1. Select **Fortify > Project Configuration**.
2. Click the **Filter Sets** tab.
3. Click **Import**.

   The Locate Template File dialog box opens.

4. Select the issue template file to import.
5. Click **Open**.

The filter sets, custom folders, and custom tags are updated.

Note: You can also click **Reset to Default** to return the settings to the default issue template.

Troubleshooting

The following topics provide information on how to troubleshoot problems you might encounter working with the Eclipse Plugin and how to report an issue to Micro Focus Fortify Customer Support.

This section contains the following topics:

Resolving the Java OutOfMemory Message

If you see the `java.lang.OutOfMemory` message while managing security content or while loading a large source code analysis results file, adjust the JVM size of the virtual machine for your IDE.

To adjust the JVM size, restart the IDE as follows:

```
eclipse.exe -vmargs -Xmx<nnn>M
```

where *<nnn>* is the amount of memory you are allocating to the IDE. For example, to allocate 300 MB to the IDE, specify `-Xmx300M`.

If you specify this option, make sure that you do not allocate more memory than is physically available. As a guideline, assuming no other memory-intensive processes are running, allocate no more than two thirds of the available memory.

Resolving Scan Failures Due to Insufficient Memory

If you run out of memory during a scan, configure project properties settings to increase the memory for that scan. (See "Configuring Analysis Settings" on page 22.)

Saving a Project That Exceeds the Maximum Removed Issues Limit

When you save a project that has more than the maximum number of removed issues, the Eclipse Complete Plugin displays following warning message:

```
Your project contains more than <RemovedIssuesLimit> removed issues.
Would you like to persist them all, or limit the number to
<RemovedIssuesLimit>?
If you limit the number, audited removed issues will take precedence of
unaudited ones.
```

Choose **Limit** to limit the number of issues to the maximum or **Save All** to save all the removed issues. The maximum number of removed issues <*RemovedIssuesLimit*> is controlled by the `com.fortify.RemovedIssuePersistanceLimit` property. See *Micro Focus Fortify Static Code Analyzer Tools Properties Reference Guide* for more information.

To configure how the Eclipse Complete Plugin handles this issue for future occurrences:

1. Select **Fortify > Options**.
2. In the left panel, select **Audit Configuration**.
3. Click the **Configuration** tab.
4. Under **Save Audit Project Options**, specify one of the following configuration settings:
   - **Limit removed issues to the maximum number**
   - **Save all removed issues every time**
   - **Prompt me next time**
5. Click **OK**.

Using the Debugging Option

If you encounter errors, you can enable the debugging option to help troubleshoot.

To enable debugging:

1. Open the `fortify.properties` file located in the following directory depending on the area you want to debug:

To debug...	Open the properties file in this location
Scanning	<*sca_install_dir*>/Core/config
Eclipse Complete Plugin	<*eclipse_install_dir*>/plugins/com.fortify.dev.ide.eclipse_<*version*>/Core/config

2. You can either enable debug mode for all Micro Focus Fortify Static Code Analyzer tools or for specific tools. Remove the comment tag (#) from in front of the property and set the value to `true`.

Property	Description
`com.fortify.Debug`	If set to `true`, all the Fortify Static Code Analyzer tools run in debug mode.
`com.fortify.awb.Debug`	If set to `true`, Fortify Audit Workbench runs in debug mode.
`com.fortify.eclipse.Debug`	If set to `true`, the Eclipse Complete Plugin runs in debug mode.

For help diagnosing the problem, provide the log files to Micro Focus Fortify Customer Support. On Windows systems, log files are in the following directories:

- `C:\Users\<username>\AppData\Local\Fortify\sca<version>\log`
- `C:\Users\<username>\AppData\Local\Fortify\Eclipse.Plugin-<version>\log`

On Linux and Unix systems, log files are in one of the following directories:

- `<userhome>/.fortify/sca<version>/log`
- `<userhome>/.fortify/Eclipse.Plugin-<version>/log`

Chapter 3: Using the Eclipse Remediation Plugin

This chapter provides an overview of the Eclipse Remediation Plugin, instructions on how to install the plugin, and how to use the plugin to audit issues associated with your Micro Focus Fortify Software Security Center applications.

Use the Eclipse Remediation Plugin to download audit results for your code from Fortify Software Security Center so that you can resolve security-related issues in Eclipse.

This section contains the following topics:

Installing the Eclipse Remediation Plugin 106

Uninstalling the Eclipse Remediation Plugin from Eclipse 108

Opening a Fortify Software Security Center Application Version 108

Remediation View 109

Locating the Source Code Associated with Issues 114

Eclipse Remediation Plugin Reports 115

Installing the Eclipse Remediation Plugin

You can install the Eclipse Remediation Plugin on Windows, Linux, and macOS systems. You can install the plugin locally or, if you set up an update site, you can install the Eclipse Remediation Plugin by connecting to the update site from Eclipse.

To update from an earlier Eclipse Remediation Plugin version, you must first remove the existing version. For information about how to uninstall the plugin, see "Uninstalling the Eclipse Remediation Plugin from Eclipse" on page 108.

Note: You do not need to specify a Fortify license file for the Eclipse Remediation Plugin. It uses the license file for Micro Focus Fortify Software Security Center, with which it works.

Installing the Eclipse Remediation Plugin Locally

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 Eclipse Remediation Plugin locally:

1. Start Eclipse.
2. Select **Help > Install New Software**.
3. Click **Add**.

   The Add Repository dialog box opens.
4. Click **Archive**, and then locate and select the `Fortify_Eclipse_Remediation_Plugin_<version>.zip` file.
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 view version and copyright information for the plugin in the **Details** box, click the plugin name.
8. Click **Next**.
9. On the **Review Licenses** step, review and accept the terms of the Micro Focus license agreement.
10. Click **Finish**.
11. To complete the installation and restart Eclipse, click **Restart Now** when prompted.

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

Installing the Eclipse Remediation Plugin from an Update Site

An alternative to requiring every developer to install the Eclipse Remediation Plugin locally is to post the plugin to an internal update site that can serve as a single distribution point. The only requirement is that you have an internal web server.

Posting the Eclipse Remediation Plugin to an Internal Update Site

To post the plugin to an internal update site:

1. Extract the contents of the Eclipse Remediation Plugin archive (`Fortify_Eclipse_Remediation_Plugin_<version>.zip`) onto your web server.
2. Provide the URL for the update site to the appropriate users.

Installing From an Update Site

To install the Eclipse Remediation Plugin from an update site:

1. Obtain the URL of the plugin update site.
2. Start Eclipse.
3. Select **Help > Install New Software**.
4. Click **Add**.

5. Do the following:
   a. In the **Name** box, type a name for the update site.
   b. In the **Location** box, type the URL for the update site.
   c. Click **OK**.

   In the Install window, the **Work with** list displays the update site you specified and the Eclipse Remediation Plugin node is listed as available software.
6. Click **Select All** and then click **Next**.
7. To view version and copyright information about the plugin in the **Details** box, click the plugin name.
8. Click **Next**.
9. On the **Review Licenses** step, review and accept the terms of the Micro Focus license agreement.
10. Click **Finish**.
11. To complete the installation, click **Yes** to restart Eclipse when prompted.

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

Uninstalling the Eclipse Remediation Plugin 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 Eclipse Remediation Plugin:

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.

Opening a Fortify Software Security Center Application Version

Because the Eclipse Remediation Plugin is designed to work with Micro Focus Fortify Software Security Center, the first thing you must do after installing it is connect to Fortify Software Security Center and open an application version.

If your server is behind a proxy, you must provide the proxy server and port as follows:

1. Select **Fortify > Options**.
2. In the **Server URL** box, type the URL for your Fortify Software Security Center server (for example, `http://111.0.0.1:8180/ssc`).
3. Type the proxy address and port number.
4. Click **OK**.

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

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

1. From Eclipse, select **Fortify > Connect to Software Security Center**.
2. Provide your Fortify Software Security Center credentials.

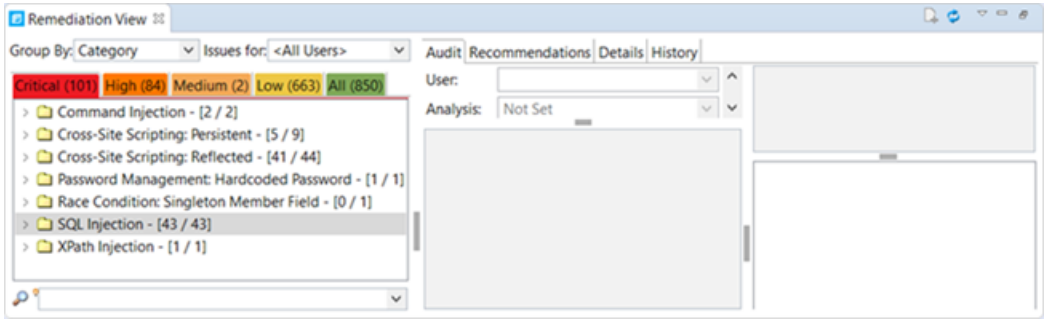
   The Select Software Security Center Application Version dialog box opens and displays a tree of Fortify Software Security Center applications and application versions.
3. Select the application version you want to open, and then click **OK**.

The Eclipse Remediation Plugin downloads the application version content from Fortify Software Security Center.

Remediation View

The Eclipse Remediation Plugin provides the security issues related to an opened application version. Issues are organized based on settings in Micro Focus Fortify Software Security Center.

The **Remediation View** displays all project issues, organized in folders (colored tabs). To the right of the issues list are four tabs that provide information specific to a selected issue in the issues list on the left.

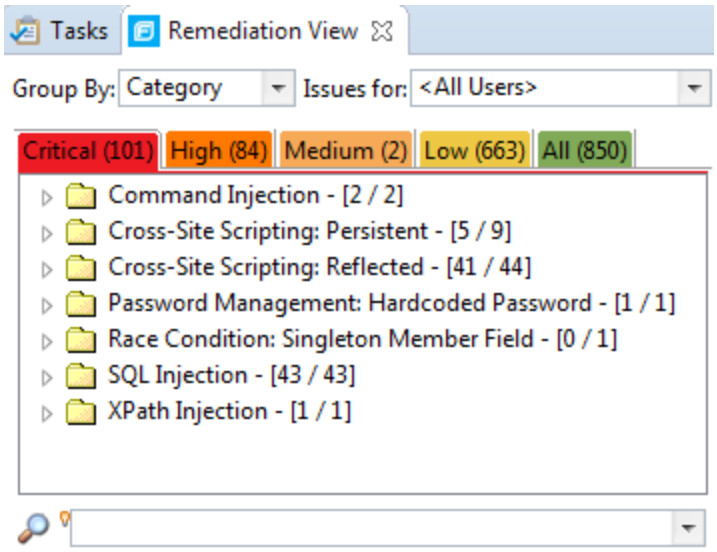


Issues List

Micro Focus Fortify Software Security Center organizes issues into folders (tabs) based on the filter sets specified in the issue template. After you select an application version to open, the Eclipse

Remediation Plugin downloads the issues for that application version and displays the **Remediation View** at the bottom of the Eclipse window.

The left portion of the **Remediation View** lists any issues assigned to you, grouped by issue category.



The issues are grouped into the following folders:

- 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.

Grouping and Viewing Issues

To view and select project issues:

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

   The default grouping is **Category**.
2. From the **Issues for** list, select one of the following:
   - **<All Users>**
   - Your Fortify Software Security Center user name
   - Possibly, additional Micro Focus Fortify Software Security Center user names
3. Click a folder (tab) to view the associated issues.

   The issue type subfolders listed on each folder (tab) are based on the **Group By** and **Issues for** values you selected.

4. To view the list of issues in a subfolder, expand the subfolder.

   The Eclipse Remediation Plugin retrieves the corresponding issues from Fortify Software Security Center.
5. Select an issue.

In the **Remediation View**, the **Issue Details** tab displays information about the selected issue.

For information about how to search for issues, see "Searching for Issues" on page 64.

Customizing the Issues List

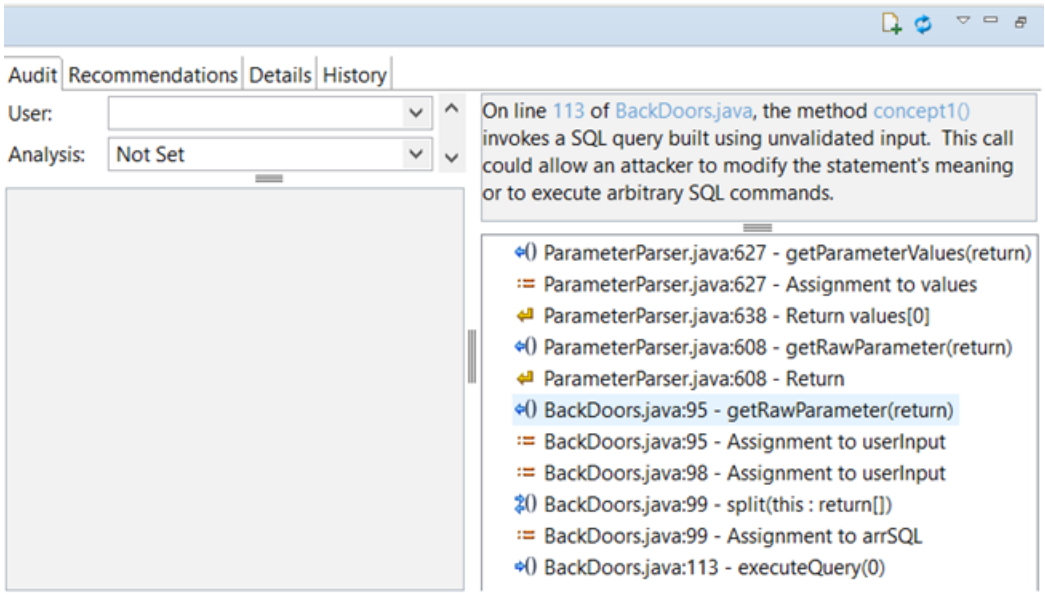
The filter sets, folders, tags, and filter settings that you see in the Remediation View are based on the issue template assigned to the application version in Micro Focus Fortify Software Security Center. You can control how the Eclipse Remediation Plugin displays issues by specifying which issue types (hidden, suppressed, and removed) to list and which filter set to apply to issues.

To customize the issues list:

1. To list a specific issue type, at the top right of the **Remediation View**, click the **View Menu** icon , click **Issue Visibility**, and then 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**.
   - To display all of 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**.

   You can select or clear each of these three options.
2. To specify the filter set to apply to issues, click the **View Menu** icon , click **Filter Set**, and then select a filter set.

Audit Tab



The **Audit** tab provides the following information for the selected issue:

- User assigned to the issue (if set)
- Analysis tag value
- Any custom tags defined for the application in Micro Focus Fortify Software Security Center
- Comments added for the issue
- Information (abstract) about the selected issue (top right)
- Analysis trace that the analyzer used to produce the results file (bottom right). For a description of the analysis trace, see "Analysis Trace View" on page 41.

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

Assigning Users to Issues

To assign a user (or a different user) to an issue:

1. From the issues list in the **Remediation View**, select an issue.
2. From the **User** list on the **Audit** tab, select the username for the user to assign to the issue.

Assigning Tags to Issues

To assign 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.

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

   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, you can click to select a date from a calendar.

Adding Comments to Issues

The comments box below the **Analysis** list displays any comments submitted for the selected issue.

To add a comment to an issue:

1. From a folder in the **Remediation View**, select an issue.
2. At the top right of the **Remediation View**, click **Add Comment**  .
   The Add Comment for Issue dialog box opens.
3. Type your comment in the text box, and then click **OK**.

Your comment is displayed in the box below the **Analysis** list and any other custom tags if they exist. The Eclipse Remediation Plugin communicates with Micro Focus Fortify Software Security Center and updates the application version on the server.

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 information on this tab.

Element	Information Provided
Recommendations/Custom Recommendations	Recommendations for particular types of issues, examples, and any custom recommendations defined for your organization.
Tips/Custom Tips	Tips for particular types of issues, including any custom tips defined for your organization.
References/Custom References	Reference information, including any custom reference defined for your organization.

Details Tab

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

Element	Information Provided
Abstract/Custom	Summary description of an issue, including custom abstracts defined by your

Element	Information Provided
Abstract	organization.
Explanation/Custom Explanation	Descriptions of the conditions in which the selected issue type occurs. This includes a discussion of the vulnerability, the constructs typically associated with it, ways in which it can be exploited, and the potential ramifications of an attack. This section also provides custom explanations defined by your organization.
Instance ID	Unique identifier for an issue
Primary Rule ID	Identifies the primary rule used to find the issue
Priority Metadata Values	Priority metadata values for the issue
Legacy Priority Metadata Values	Legacy priority metadata values for the issue
Remediation Effort	The relative amount of effort required to fix and verify an issue.

History Tab

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

Locating the Source Code Associated with Issues

You can use the Eclipse Remediation Plugin to locate security-related issues in your code.

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

1. Make sure that you have the same application version open in both Eclipse and the Eclipse Remediation Plugin.

   Note: The name of the Eclipse project and the Micro Focus Fortify Software Security Center application must be the same.

2. Select an issue in the issue tree or select a line in the analysis trace section of the **Remediation View**.

Eclipse displays the associated line of code.

Eclipse Remediation Plugin Reports

You can generate reports on the Micro Focus Fortify Software Security Center from the Eclipse Remediation Plugin. You can also download a report that has already been created from 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. For more information, see "Opening a Fortify Software Security Center Application Version" on page 108.

Generating Reports

To generate a report:

1. Select **Fortify > Generate Report**.
   The Select Software Security Center Application Version dialog box opens.
2. Select an application version and then click **OK**.
   The Software Security Center Report Generation dialog box opens.
3. Select a report type from the list.
4. 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.
5. To specify the file name for the report and select the report format (PDF, DOC, or XLS), click **Report details**.
   The default report format is PDF.
6. Click **Generate**.
7. 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 on Micro Focus 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**.

Send Documentation Feedback

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

Feedback on Installation and Usage Guide (Fortify Plugins for Eclipse 19.2.0)

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@microfocus.com.

We appreciate your feedback!