opentext™

OpenText™ Fortify Plugin for Eclipse

Software Version: 24.4.0

User Guide

Document Release Date: October 2024
Software Release Date: October 2024

Legal Notices

Open Text Corporation

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

Copyright Notice

Trademark Notices

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 10, 2024. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

Contents

Preface

Contacting Customer Support

Visit the Support website to:

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

https://www.microfocus.com/support

For More Information

For more information about Fortify software products:

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

About the Documentation Set

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

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

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

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

Fortify Product Feature Videos

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

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

Change Log

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

Software Release / Document Version	Change
24.4.0	Updated: • You can use the encoded authentication token when connecting to Fortify Software Security Center as the decoded token format is deprecated (see "Logging in to Fortify Software Security Center" on page 24)
24.2.0	Added: • "Integration with Fortify ScanCentral SAST" on page 12 Updated: • Added instructions for installing the Fortify Plugin for Eclipse from the Eclipse Marketplace (see "Installing the Fortify Eclipse Complete Plugin" on page 17) • Added timeout setting for downloading analysis results from Fortify Software Security Center (see "Configuring a Connection to Fortify Software Security Center" on page 24) • Added how to use a standalone Fortify ScanCentral SAST client (see "About Scanning with Fortify ScanCentral SAST" on page 33, and "Configuring Fortify ScanCentral SAST Options" on page 35) • The unused metric, executable lines of code, is no longer displayed in the Project Summary view (see "Project Summary View" on page 54) • Added search modifier `engine priority` (see "Search Modifiers" on page 72) • Added New Issue by Category grouping attribute (see "Grouping Issues" on page 98)
23.2.0	Added: • "Integration with Fortify Static Code Analyzer" on page 12

Software Release / Document Version	Change
23.1.0	Updated: • Changes were made throughout this guide for the introduction of a separate OpenText™ Fortify Static Code Analyzer Applications and Tools installer • New location for sample bug tracker plugins (see "Integrating with a Bug Tracker Application" on page 114)

Chapter 1: Introduction

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

This section contains the following topics:

Fortify Plugin for Eclipse

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

- Analysis—Enables you to start an OpenText™ Fortify Static Code Analyzer analysis with Fortify Software Security Content, view the analysis results, and fix the code associated with uncovered issues, all within the Eclipse IDE.
- Audit—Enables you to open existing analysis results (also called *audit projects*) 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 go to the source code location associated with each vulnerability, and then prioritize and audit the results.

  Note: If your Fortify license restricts auditing, then you can scan your code, view audit projects (FPR files), and generate reports from the Fortify Plugin for Eclipse, but you cannot audit issues or make any changes to the audit project.

- Collaboration—Includes server-related functionality such as connecting to OpenText™ Fortify Software Security Center, uploading analysis results, and performing collaborative audits. (If you do not want this functionality, then there is no need to install the collaboration plugin.)

  Note: If your Fortify license restricts auditing, then you can open and review collaborative audits in Fortify Software Security Center, but you cannot make any changes. You also cannot upload audit projects to Fortify Software Security Center.

Note: For information about supported versions of Eclipse, see the *Fortify Software System Requirements* document.

Audit Projects and Issue Templates

After you initiate a source code scan from the Fortify Plugin for Eclipse, Fortify Static Code Analyzer scans and analyzes the code to produce comprehensive results (referred to as an audit project).

In Fortify Software Security Center, an application is a codebase that serves as a container for one or more application versions. A Fortify Software Security Center application version is an instance of the codebase that will eventually be deployed. An audit project is comparable to a Fortify Software Security Center application version in that it represents a snapshot of the codebase.

Issue templates determine how the Fortify Plugin for Eclipse (and Fortify Software Security Center) configures and prioritizes the vulnerabilities (issues) uncovered in source code. The Fortify Plugin for Eclipse comes with a single basic issue template, which you can use as is, or modify to suit your project needs. You can also import an issue template from Fortify Software Security Center, or create a new issue template from the Fortify Plugin for Eclipse.

Integration with Fortify Static Code Analyzer

If you installed the analysis plugin component, you can start a local Fortify Static Code Analyzer analysis of your source code from Eclipse. You install Fortify Static Code Analyzer separately from the applications and tools. For instructions on installing Fortify Static Code Analyzer, see the *OpenText™ Fortify Static Code Analyzer User Guide*. Updating Fortify Software Security Content also requires a local installation of Fortify Static Code Analyzer.

The Fortify Applications and Tools installer (which includes the Fortify Plugin for Eclipse) can detect an existing Fortify Static Code Analyzer that is locally installed in the default location or in the same root folder where you installed Fortify Applications and Tools. If necessary, you are prompted when you first attempt to analyze your code to select the location of a locally installed Fortify Static Code Analyzer.

See Also

"About Scanning Locally" on page 27

Integration with Fortify ScanCentral SAST

To scan your code using OpenText™ Fortify ScanCentral SAST, you must have a local Fortify ScanCentral SAST client and a properly configured Fortify ScanCentral SAST installation.

You can install Fortify ScanCentral SAST client, as a component with either the Fortify Static Code Analyzer or the Fortify Applications and Tools installation or from a Fortify ScanCentral SAST ZIP archive.

See Also

"About Scanning with Fortify ScanCentral SAST" on page 33

Integration with Fortify Software Security Center

Fortify Software Security Center provides a web portal that developers, managers, and security teams can use to share, collaborate, and track remediation of the potential vulnerabilities that Fortify Static Code Analyzer scans uncover. If you connect the Fortify Plugin for Eclipse to your Fortify Software Security Center server, you can upload and merge your scan and audit results and share them with your team. This enables you to monitor trends and indicators across multiple application versions.

Integration with Fortify Software Security Center enables you to:

- Upload audit projects (FPR files)
- Perform collaborative application audits
- Manage the security content, which consists of Fortify Secure Coding Rulepacks, custom Rulepacks, and external metadata applied during Fortify Static Code Analyzer scans
- Download issue templates
- Upload new and modified issue templates

See Also

"Working with Fortify Software Security Center" on page 23

"Configuring a Connection to Fortify Software Security Center" on page 24

Related Documents

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

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

All Products

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

Document / File Name	Description
About Fortify Software Documentation About_Fortify_Docs_<*version*>.pdf	This paper provides information about how to access Fortify product documentation. **Note:** This document is included only with the product download.

Document / File Name	Description
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.
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 Fortify Software <version> Fortify_Whats_New_<*version*>.pdf	This document describes the new features in Fortify Software products.

Fortify ScanCentral SAST

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

Document / File Name	Description
OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide SC_SAST_Guide_<*version*>.pdf	This document provides information about how to install, configure, and use Fortify ScanCentral SAST to streamline the static code analysis process. It is written for anyone who intends to install, configure, or use Fortify ScanCentral SAST to offload the resource-intensive translation and scanning phases of their Fortify Static Code Analyzer process.

Fortify Software Security Center

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

Document / File Name	Description
OpenText™ Fortify Software Security Center User Guide	This document provides Fortify Software Security Center users with detailed information about how to deploy and use

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

Fortify Static Code Analyzer

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

Document / File Name	Description
OpenText™ 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.
OpenText™ 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.
OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide LIM_Guide_<*version*>.pdf	This document describes how to install, configure, and use the Fortify License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.

Fortify Static Code Analyzer Applications and Tools

The following documents provide information about Fortify Static Code Analyzer applications and tools. These documents are available on the Product Documentation website at

https://www.microfocus.com/documentation/fortify-static-code-analyzer-and-tools.

Document / File Name	Description
OpenText™ Fortify Static Code Analyzer Applications and Tools Guide SCA_Apps_Tools_<*version*>.pdf	This document describes how to install Fortify Static Code Analyzer applications and tools. It provides an overview of the applications and command-line tools that enable you to scan your code with Fortify Static Code Analyzer, review analysis results, work with analysis results files, and more.
OpenText™ Fortify Audit Workbench User Guide AWB_Guide_<*version*>.pdf	This document describes how to use Fortify Audit Workbench to scan software projects and audit analysis results. This guide also includes how to integrate with bug trackers, produce reports, and perform collaborative auditing.
OpenText™ Fortify Plugin for Eclipse User Guide Eclipse_Plugin_Guide_<*version*>.pdf	This document provides information about how to install and use the Fortify Plugin for Eclipse to analyze and audit your code.
OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studio User Guide IntelliJ_AnalysisPlugin_Guide_<*version*>.pdf	This document describes how to install and use the Fortify Analysis Plugin for IntelliJ IDEA and Android Studio to analyze your code and optionally upload the results to Fortify Software Security Center.
OpenText™ Fortify Extension for Visual Studio User Guide VS_Ext_Guide_<*version*>.pdf	This document provides information about how to install and use the Fortify Extension for Visual Studio to analyze, audit, and remediate your code to resolve security-related issues in solutions and projects.

Chapter 2: Getting Started

The following topics describe how to install and update the Fortify Plugin for Eclipse, update Fortify security content, and connect to Fortify Software Security Center.

This section contains the following topics:

Installing the Fortify Eclipse Complete Plugin

You can install the Fortify Eclipse Complete Plugin from either the Eclipse Marketplace or from the plugin component installed with Fortify Applications and Tools.

To update from an earlier Fortify Eclipse Complete Plugin version, you must first remove the existing version.

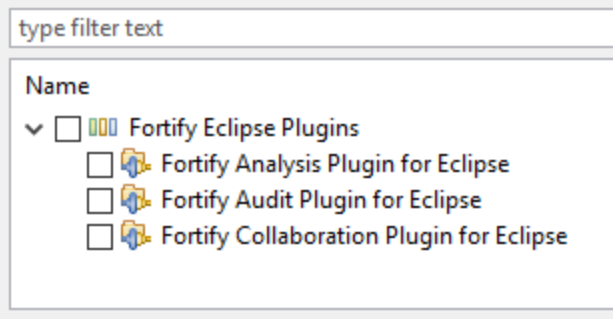
Note: These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.

To install the Fortify Eclipse Complete Plugin locally:

1. Start Eclipse.
2. Select **Help > Install New Software**.
3. Click **Add**.
4. (Optional) In the **Name** box, type a name for your local repository.
5. Select the Fortify Plugin for Eclipse to install by doing one of the following:
   - To install the plugin from the Eclipse Marketplace, in the **Location** box type `https://tools.fortify.com/fortifyeclipseplugin`.

     Note: You might need to configure a proxy in Eclipse to reach the location.
   - To install the plugin from a Fortify Applications and Tools installation, click **Archive**, browse to and select the `<tools_install_dir>/plugins/eclipse/Fortify_Eclipse_Complete_Plugin_<version>.zip` file, and then click **Open**.
6. Click **Add**.

7. 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.

8. 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.

9. Click **Next**.
10. To display version and copyright information for a plugin in the **Details** section, click the feature name.
11. Click **Next**.
12. On the **Review Licenses** page, review and accept the terms of the license agreement.
13. Click **Finish**.
14. To complete the installation and restart Eclipse, click **Restart Now** when prompted.

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

About Reinstalling After Upgrading Fortify Applications and Tools from Fortify Audit Workbench

If you have upgraded Fortify Static Code Analyzer applications and tools from OpenText™ Fortify Audit Workbench, you must uninstall, and then reinstall the Fortify Plugin for Eclipse. For information about how you can upgrade the Fortify Static Code Analyzer applications and tools from Fortify Audit Workbench, see the *OpenText™ Fortify Audit Workbench User Guide*.

Fortify Software Security Content

Fortify Static Code Analyzer 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)

OpenText provides the ability to write custom rules that add to the functionality of Fortify Static Code Analyzer and the Fortify 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 Fortify 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 *OpenText™ Fortify Static Code Analyzer Custom Rules Guide*.

If you are using collaborative auditing with Fortify Software Security Center, make sure that any custom rules or external metadata changes are also made in Fortify Software Security Center.

You must have security content on your local system to run a scan locally or to use Fortify ScanCentral SAST and run the translation locally (see "Analyzing the Source Code" on page 27). Typically, you obtain the current Fortify Software Security Content when you install Fortify Static Code Analyzer.

See Also

- "Configuring Security Content Updates" below
- "Updating Security Content" on page 21
- "Importing Custom Security Content" on page 23

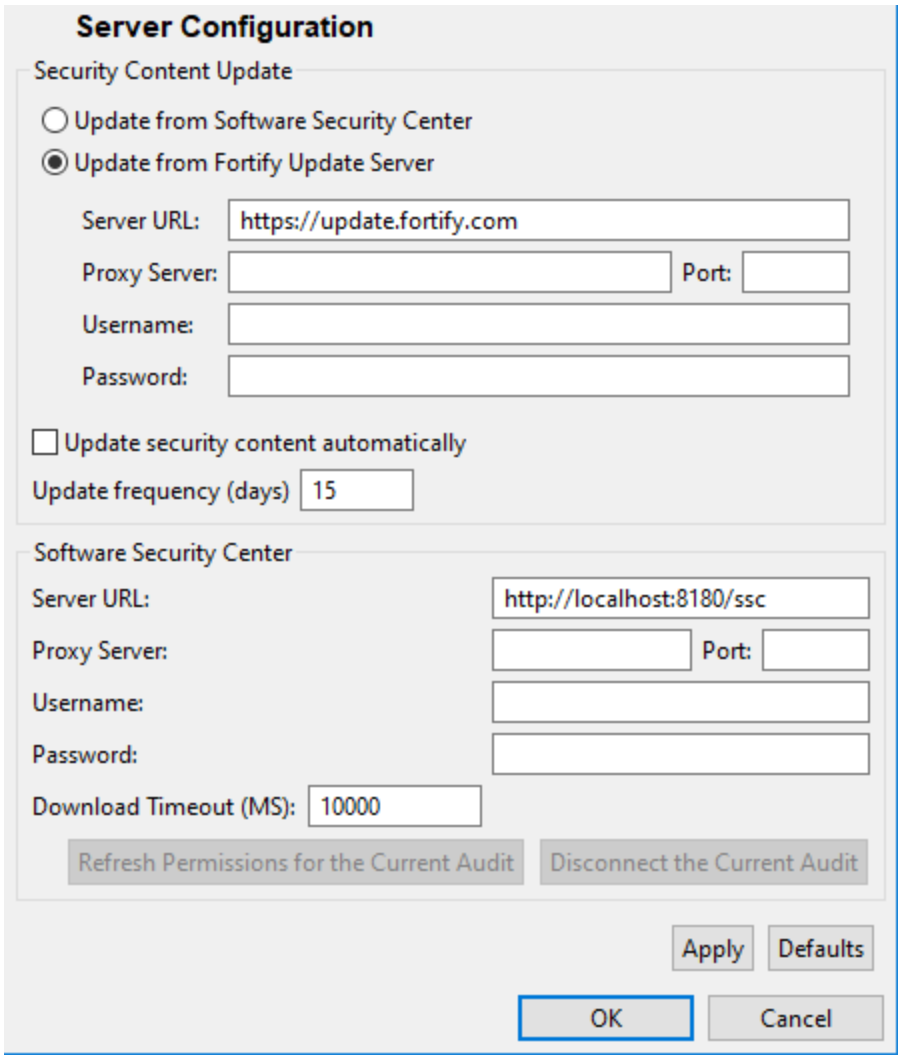
Configuring Security Content Updates

If the analysis plugin component is installed, you can configure the server from which to update security content and whether to have the security content updated from a server automatically.

To update security content from your local system (if you do not have an internet connection or a Fortify Software Security Center server), see "Updating Security Content" on page 21.

To configure the server from where you will obtain security content:

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



3. To update security content from your Fortify Software Security Center server:
   a. Under **Security Content Update**, select **Update from Software Security Center**.
   b. Under **Software Security Center**, specify the Fortify Software Security Center server web address and if required, the proxy server, port number, and credentials for proxy authentication.

      Note: When you specify proxy information, exclude the protocol from the proxy server (for example, some.secureproxy.com). You must specify a proxy port number.

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 web address for the update server.
   b. If required, specify the proxy server, port number, and credentials for proxy authentication.

      Note: When you specify proxy information, exclude the protocol from the proxy server (for example, some.secureproxy.com). You must specify a proxy port number.

5. To update security content from a server automatically and with a specific frequency:
   a. Select the **Update security content automatically** check box.
   b. In the **Update frequency (days)** box, specify how often to update the security content.
6. Click **OK**.

See Also

"Updating Security Content" below

"Importing Custom Security Content" on page 23

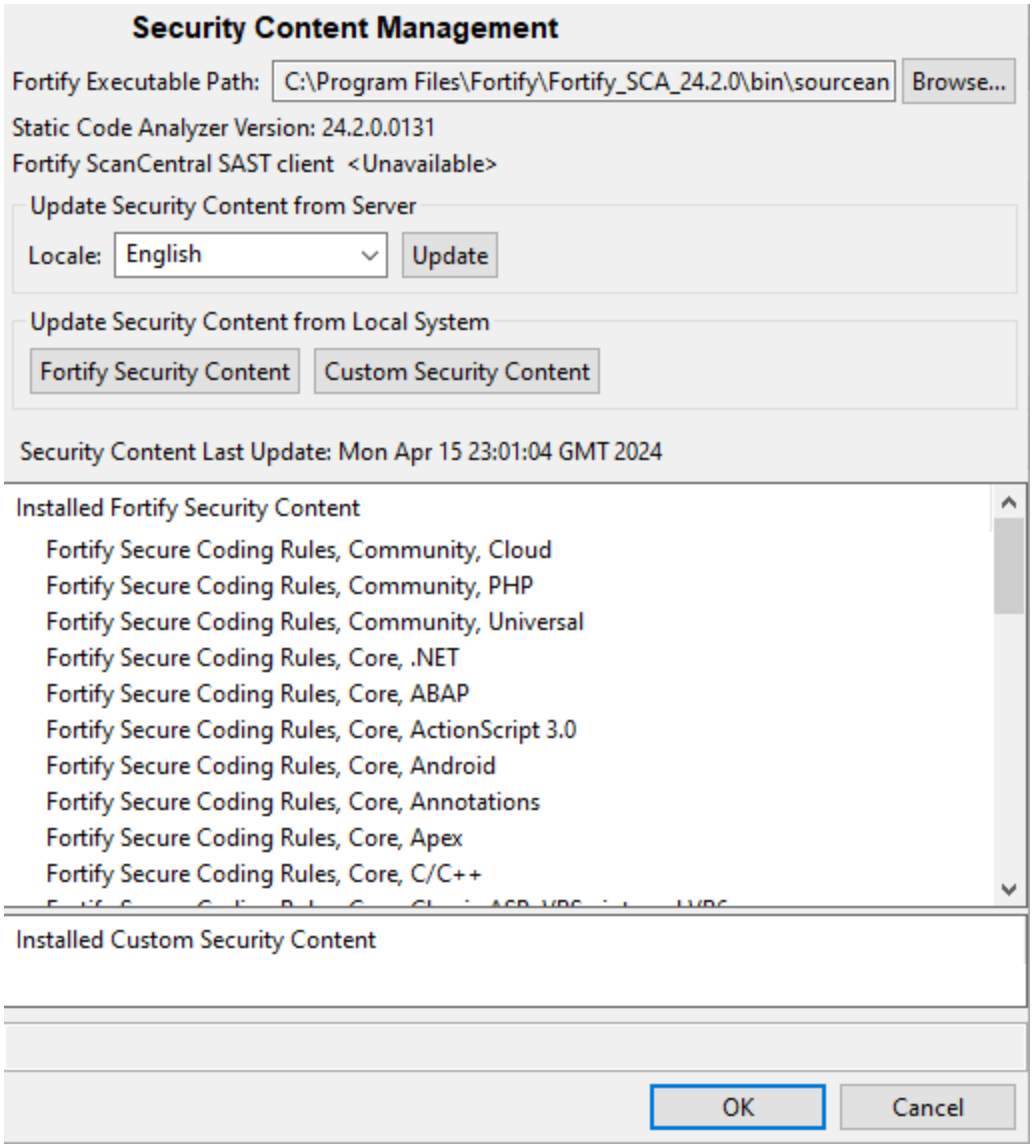
Updating Security Content

To optimize the Fortify Eclipse Complete Plugin functionality to scan with Fortify Static Code Analyzer, you must have up-to-date security content. You can update Fortify security content from a configured server or from your local system.

Important! To update security content, you must have Fortify Static Code Analyzer locally installed.

To update security content:

1. Select **Fortify > Options**.
2. In the left pane, 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. You must provide the location of a locally installed Fortify Static Code Analyzer. If the **Fortify Executable Path** shows **<Unavailable>**, do the following:
   a. Click **Browse** to the right of **Fortify Executable Path**.
   b. Go to the Fortify Static Code Analyzer installation directory and select the executable file.

Make sure to set the file type to **sourceanalyzer executable**.

c. Click **OK**.

4. To update Fortify security content from a server, do the following:
   a. (Optional) From the **Locale** list, select a language.

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

   b. Click **Update**.
5. To update Fortify security content from your local system, under **Update Security Content from Local System**, do the following:
   a. Click **Fortify Security Content**.
   b. Navigate to a Fortify security content ZIP file, and then click **Open**.

All existing security content is replaced with the selected Fortify security content. Any existing custom security content is unchanged.

See Also

"Importing Custom Security Content" below

"Configuring Security Content Updates" on page 19

Importing Custom Security Content

You can import custom security content to use in local analysis.

Note: To import custom external metadata, you must 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 pane, select **Security Content Management**.
3. Under **Update Security Content from Local System**, click **Custom Security Content**.
4. Select the custom rules files to import (*.xml and *.bin), and then click **Open**.

Working with Fortify Software Security Center

You need to configure a connection to Fortify Software Security Center to accomplish any of the following tasks:

- Upload your scan results to Fortify Software Security Center
- Audit applications collaboratively using Fortify Software Security Center
- Update your Fortify Software Security Content from Fortify Software Security Center

Configuring a Connection to Fortify Software Security Center

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

- The web address for your Fortify Software Security Center and if necessary, the proxy server and port number for the connection
- If you 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 for Eclipse.
- If your Fortify Software Security Center server uses an SSL connection from an internal certificate authority or a self-signed certificate, you must import a self- or locally-signed certificate into the Java Keystore for Eclipse.

To configure a connection to Fortify Software Security Center:

1. Select **Fortify > Options**.
2. In the left pane, select **Server Configuration**.
3. Under **Software Security Center Configuration**, specify the **Server URL** for your Fortify Software Security Center server.
4. If required, specify the proxy server, port number, and optionally credentials for proxy authentication.
5. To change the length of time provided to download analysis results from Fortify Software Security Center, type the timeout value in milliseconds in the **Download Timeout** box.

   Setting a value of zero is equivalent to no timeout for the download of analysis results.
6. Click **OK**.

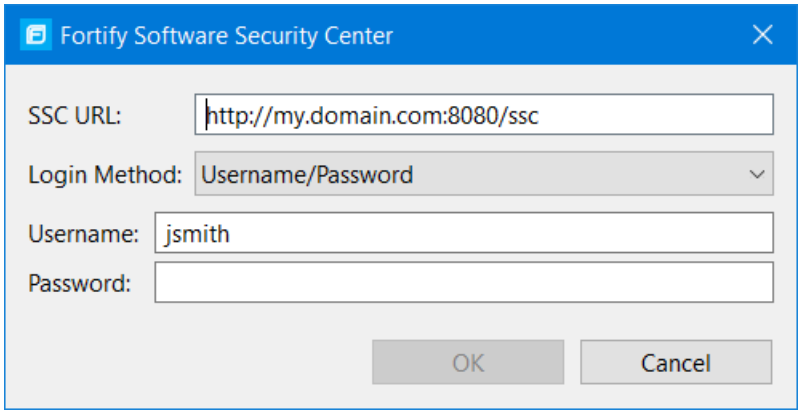
Logging in to Fortify Software Security Center

The first time you perform an operation that requires a connection to Fortify Software Security Center such as uploading analysis results or performing a collaborative audit, you are prompted to log in.

To log in to Fortify Software Security Center:

1. If you have not configured a connection to Fortify Software Security Center, in the **SSC URL** box, type the server web address.

2. From the **Login Method** list, select the login method set up for you in Fortify Software Security Center.



3. Depending on the selected login method, do one of the following:

Login method	Procedure
Username/Password	Type your Fortify Software Security Center user name and password.
Authentication Token	In the **Token** box, specify the encoded value of a Fortify Software Security Center authentication token of type ToolsConnectToken. **Note:** For instructions about how to create an authentication token, see the *OpenText™ Fortify Software Security Center User Guide*.
X.509 SSO	a. Click **Browse** 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.

4. 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 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 *OpenText™ Fortify Software Security Center User Guide*.

To enable or disable synchronization to the server:

1. Select **Fortify > Options**.
2. In the left pane, click **Default Project Configuration**.
3. Select the **Synchronize Options** tab.
4. To enable synchronization to the server, select **Synchronize project with server**.

See Also

"Scheduling Synchronization" below

Scheduling Synchronization

You can customize which action synchronizes your local version of a project with the Fortify Software Security Center 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**.

Chapter 3: Analyzing the Source Code

If you installed the analysis plugin component, you can start an analysis of your source code from Eclipse. To get the best analysis results, make sure that you can compile the project with no errors before you analyze your project source code. A security analysis with Fortify Static Code Analyzer consists of the following main phases:

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

There are two ways to analyze your source code:

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

  After the scan is complete, the Fortify Plugin for Eclipse displays the analysis results in Eclipse.
- Use Fortify ScanCentral SAST to perform the entire analysis (translation and scan phases) or only the scan phase. For information about how to configure and run the analysis using Fortify ScanCentral SAST, see "About Scanning with Fortify ScanCentral SAST" on page 33.

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

  To view the analysis results after a Fortify ScanCentral SAST scan, configure the Fortify Plugin for Eclipse to upload the analysis results to a Fortify Software Security Center server. You can then view the analysis results in Fortify Software Security Center, or you can use the Fortify Remediation Plugin for Eclipse to view them in Eclipse.

  Alternatively, use the provided job token in the Fortify ScanCentral SAST command-line interface to retrieve the analysis results (FPR) file (see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*). You can then use the Fortify Plugin for Eclipse to open the analysis results in Eclipse (see "Opening an Audit Project" on page 105).

This section contains the following topics:

About Scanning Locally

This section describes how to perform a scan of your source code on the local system. You must provide the Fortify Eclipse Complete Plugin with the location of a locally installed Fortify Static Code

Analyzer. You are prompted for the location of Fortify Static Code Analyzer the first time you analyze your project locally The Fortify Eclipse Complete Plugin invokes Fortify Static Code Analyzer with the server Java Virtual Machine.

OpenText strongly recommends that you periodically update the security content, which contains Fortify Secure Coding Rulepacks and external metadata. For instructions, see "Updating Security Content" on page 21.

About Quick Scan Mode

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

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

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

You can use quick scan mode for scans that use a locally installed Fortify Static Code Analyzer. Audit quick scan results just as you audit full analysis results. To configure your scan to run in full scan or quick scan mode, see "Configuring Advanced Local Analysis Options" on the next page.

Configuring Local Analysis Options

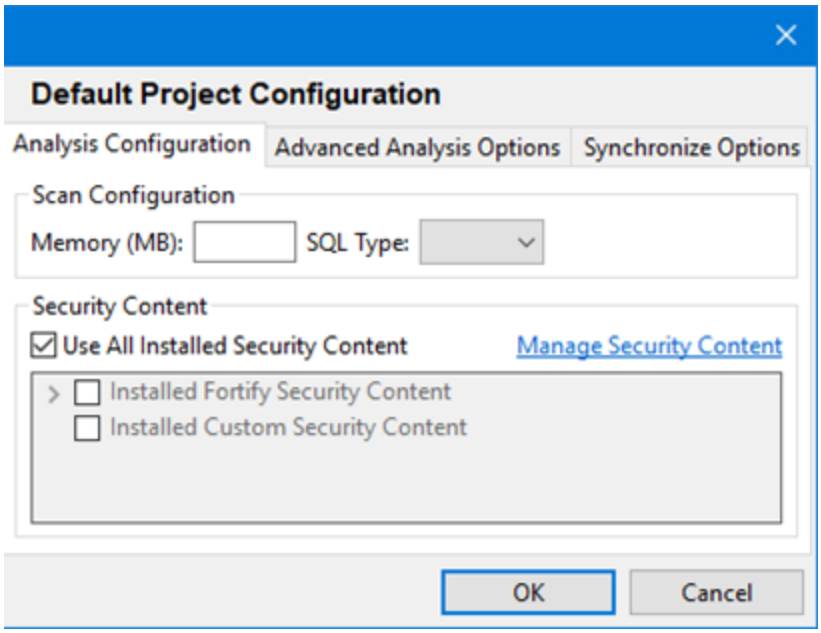
The analysis options enable you to customize the security content and the amount of memory Fortify Static Code Analyzer uses during a local analysis. You can also specify the SQL type in your project. The source code analysis options are available only if the analysis plugin is installed.

To configure the analysis options:

1. Select **Fortify > Options**.
2. In the left pane, select **Default Project Configuration**.

   The **Analysis Configuration** tab opens.

   Note: This configuration requires that you specify local installation path for Fortify Static Code Analyzer. You can configure the location of the Fortify Static Code Analyzer executable file on the Security Content Management page.



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, from the **SQL Type** list, select **TSQL** or **PLSQL**.

   Note: The **SQL Type** option notifies Fortify Static Code Analyzer about the SQL type that the project uses. SQL code is only scanned if it is included in the project.

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**.

   For more information, see "Updating Security Content" on page 21.
7. Click **OK**.

Configuring Advanced Local Analysis Options

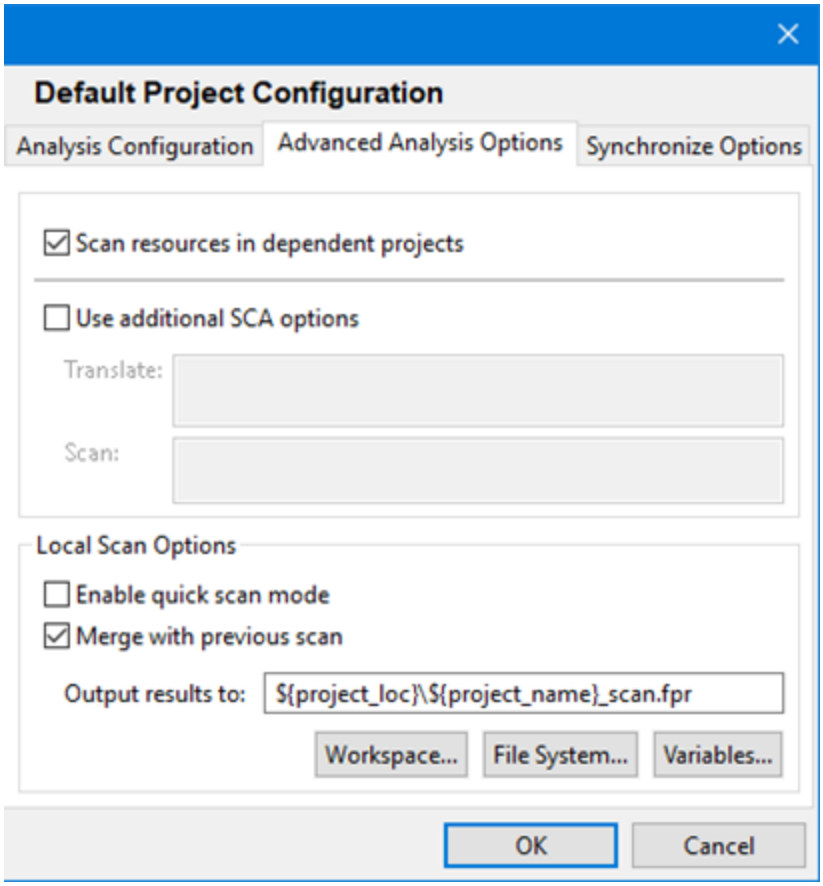
Use the advanced analysis options to customize Fortify Static Code Analyzer translation and scan command-line options. You can also specify whether quick scan mode is enabled, if issues are merged during a rescan, if resources in dependent projects are scanned, and the location for the analysis results file. These options are available only if the analysis plugin is installed.

To change the advanced analysis options:

1. Select **Fortify > Options**.
2. In the left pane, select **Default Project Configuration**.

3. Select the **Advanced Analysis Options** tab.

   Note: This configuration requires that you specify local installation path for Fortify Static Code Analyzer. You can configure the location of the Fortify Static Code Analyzer executable file on the **Security Content Management** page.



4. To scan only the selected project, clear the **Scan resources in dependent projects** check box.

   By default, the Fortify Plugin for Eclipse includes all source files from dependent projects in scans of selected projects. For more information, see "Viewing the Resources and Classpath to be Scanned" on the next page.

5. Select the **Use additional SCA options** check box and 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 the proper syntax, see the *OpenText™ Fortify Static Code Analyzer User Guide*.

6. To perform a quick scan, select the **Enable quick scan mode** check box.

   For more information about quick scans, see "About Quick Scan Mode" on page 28.

7. To disable merging the results of the next scan you run with results from the previous scan, clear the **Merge with previous scan** check box.

   For more information about merging analysis results with rescanning, see "Rescanning Projects" on the next page.
8. To change the default directory and FPR file name for all projects, 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 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 FPR files.

   To change the default directory and FPR file name for a specific project, use the Eclipse Properties window (see "Configuring Analysis Options for Specific Projects" below).
9. Click **OK** to save the advanced analysis options.

Configuring Analysis Options for Specific Projects

To specify Fortify Static Code Analyzer analysis options a specific project:

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

   The Properties for <*project_name*> window opens.
2. In the left pane, select **Fortify Project Properties**.
3. Select the **Enable project specific settings** check box.
4. Make the changes you want for this specific project.

   For descriptions of the options, see "Configuring Local Analysis Options" on page 28 and "Configuring Advanced Local Analysis Options" on page 29.

Viewing the Resources and Classpath to be Scanned

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

1. From the Java view in Eclipse, do one of the following:
   - Right-click the project name, and then select **Advanced Analysis**.
   - 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 complete absolute path of the project resources and the class path files to be scanned. If you have **Scan resources in dependent projects** enabled in the

default project configuration options (see "Configuring Advanced Local Analysis Options" on page 29), you can see any dependent projects in the **Scanning Resources** root. All library JAR files configured for your project are shown in the **Classpath** folder.

Scanning Projects Locally

The Fortify Plugin for Eclipse 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: To scan projects that have special translation or build conditions or have files you want to exclude from the project, use the advanced analysis (see "Running an Advanced Analysis" on page 38).

To scan a project:

1. Open the project in the Java perspective.
2. In the **Package Explorer** or **Project Explorer** view, right-click the project, and then select **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: OpenText does not recommend this scan method, because analysis results are more accurate when an entire project is scanned together.

To scan individual files or packages:

1. 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**.

Rescanning Projects

By default, when you rescan a project from Eclipse, the scan merges the results from the previous scan with the results from the new scan. This enables you to see specifically which issues have been fixed and which issues were introduced since the earlier scan. You can enable or disable the merging of scan results. If you disable merging analysis results, then the existing analysis results file is overwritten with the new analysis results.

Disabling Merging Scan Results for all Projects

To disable merging the results of the next scan you run with results from the previous scan as the default for all projects:

1. Select **Fortify > Options**.
2. In the left pane, select **Default Project Configuration**.
3. Select the **Advanced Analysis Options** tab.
4. Under **Local Scan Options** section, clear the **Merge with previous scan** check box.
5. Click **OK**.

Note: You can override this merging option for a specific project by configuring project properties. For more information, see "Disabling Merging Scan Results for a Specific Project" below.

You can specify whether to merge the results with the previous scan results on a per-scan bases using an advanced scan (see "Running an Advanced Analysis" on page 38).

Disabling Merging Scan Results for a Specific Project

You can override merging for a specific project.

To disable Fortify Plugin for Eclipse from merging scan results for a specific project:

1. From the Java perspective, right-click a project name, and then select **Properties**.
2. In the left pane, select **Fortify Project Properties**.
3. Select the **Enable project specific settings** check box.
4. Select the **Advanced Analysis Options** tab.
5. Under **Local Scan Options**, clear the **Merge with previous scan** check box.
6. Click **Apply and Close**.

About Scanning with Fortify ScanCentral SAST

This topic describes the requirements for using Fortify ScanCentral SAST to analyze your code and to upload the analysis results to Fortify Software Security Center. For instructions about how to configure the Fortify ScanCentral SAST options, see "Configuring Fortify ScanCentral SAST Options" on page 35.

With Fortify Plugin for Eclipse, you can either:

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

You must translate the project locally if it uses a language that Fortify ScanCentral SAST does not support for remote translation (see *Fortify Software System Requirements*).

Make sure that the Fortify Software Security Content version on the local system is the same as the version on the Fortify ScanCentral sensor. OpenText strongly recommends that you periodically update the security content. For information about how to update the security content locally, see "Updating Security Content" on page 21. Use the fortifyupdate utility to update security content on the ScanCentral sensor (see the *OpenText™ Fortify Static Code Analyzer User Guide*).

See Also

"Requirements to Scan with Fortify ScanCentral SAST" below

Requirements to Scan with Fortify ScanCentral SAST

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

- A local copy of a Fortify ScanCentral SAST client

  For information on how to obtain a Fortify ScanCentral SAST client, see "Integration with Fortify ScanCentral SAST" on page 12.
- A properly configured Fortify ScanCentral SAST installation

  Make sure the configuration for your Fortify ScanCentral SAST client is properly authorized with a client authentication token that matches the setting for the Fortify ScanCentral SAST Controller. For more information, see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.
- To connect to Fortify ScanCentral SAST, you need either:
  - A ScanCentral SAST Controller URL

    Important! If the ScanCentral SAST Controller uses an SSL connection from an internal certificate authority or a self-signed certificate, you must add the certificate to the Java Keystore depending on the location of the Fortify ScanCentral SAST client:

    - Installed with Fortify Static Code Analyzer: `(missing or bad snippet)/jre/lib/security/cacerts`
    - Installed with Fortify Applications and Tools: `(missing or bad snippet)/jre/lib/security/cacerts`
    - Standalone Fortify ScanCentral SAST client: `<java_home_dir>/lib/security/cacerts`
  - A Fortify Software Security Center URL and an authentication token of type ToolsConnectToken

    To configure the Fortify Software Security Center URL, see "Configuring a Connection to Fortify Software Security Center" on page 24. For instructions on how to create an authentication token, see the *OpenText™ Fortify Software Security Center User Guide*.

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

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

  Note: OpenText recommends that the Fortify Software Security Center URL configured in the Server Configuration options matches the Fortify Software Security Center server integrated with the ScanCentral SAST Controller.

- A Fortify Software Security Center authentication token of type ToolsConnectToken

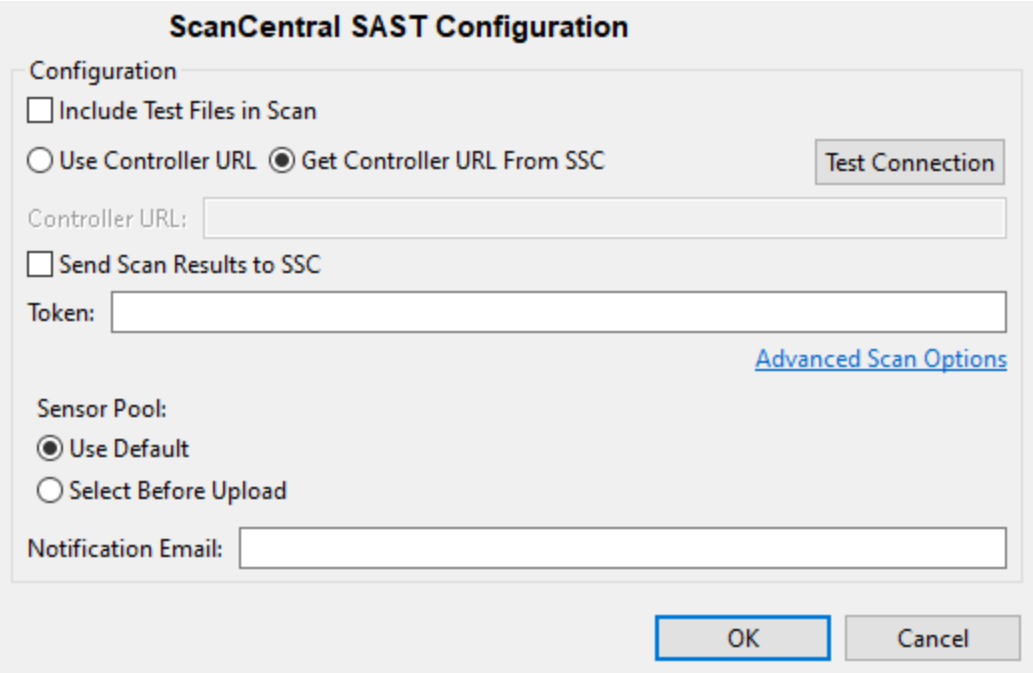
  For instructions on how to create an authentication token, see the *OpenText™ Fortify Software Security Center User Guide*.
- An application version that exists in Fortify Software Security Center
- Permission to access the application version where you want to upload analysis results

Configuring Fortify ScanCentral SAST Options

This section describes how to configure the default Fortify ScanCentral SAST options to use when you submit a project for analysis. You can specify how to connect to the Fortify ScanCentral SAST Controller, whether to upload analysis results to Fortify Software Security Center, and other Fortify ScanCentral SAST settings such as inclusion of test files, sensor pool selection, and notification email address). You can also specify Fortify Static Code Analyzer translation and scan options to include in the analysis.

To configure the Fortify ScanCentral SAST options:

1. Select **Fortify > Options**.
2. To configure the Fortify ScanCentral SAST client location:
   a. In the left pane, select **Security Content Management**.
   b. To the right of the **Fortify Executable Path** box, click **Browse**, and do one of the following:
      - If you installed Fortify Static Code Analyzer that includes an embedded Fortify ScanCentral SAST client, go to *<sca_install_dir>*/bin/ and select `sourceanalyzer.exe` (on Windows) or `sourceanalyzer` (on non-Windows).
      - To select a standalone client installed with Fortify Applications and Tools, change the file type to **ScanCentral**, and then go to *<tools_install_dir>*/bin/ and select `scancentral.bat` (on Windows) or `scancentral` (on non-Windows).
      - To select a standalone client installed in a different location, change the file type to **ScanCentral**, and then select `scancentral.bat` (on Windows) or `scancentral` (on non-Windows).
3. In the left pane, select **ScanCentral SAST Configuration**.



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

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

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

     Make sure that you have the Fortify Software Security Center URL that is associated with the ScanCentral SAST Controller provided in the **Server Configuration** options (see "Configuring a Connection to Fortify Software Security Center" on page 24).

     Tip: Click **Test Connection** to confirm that the URL and token is valid, and the server is accessible.
6. To upload the analysis results to Fortify Software Security Center, select the **Send Scan Results to SSC** check box.

   If you have not already specified a Fortify Software Security Center authentication token, do the following:
   - In the **Token** box, paste the decoded token value for an authentication token of type ToolsConnectToken.

Note: If you connect to Fortify ScanCentral SAST using a Controller URL, analysis results are uploaded to the Fortify Software Security Center server specifically integrated with the ScanCentral SAST Controller.

7. (Optional) To specify Fortify Static Code Analyzer command-line options for the translation or scan phase (or to specify whether to scan resources in dependent projects):
   a. Click **Advanced Scan Options**.
   b. Select the **Advanced Analysis Options** tab.
   c. Select the **Use additional SCA options** check box and type Fortify Static Code Analyzer command-line options for the translation or scan phase. For detailed information about the available Fortify Static Code Analyzer options and the proper syntax, see the *OpenText™ Fortify Static Code Analyzer User Guide*.
   d. Click **OK**.
8. Under **Sensor Pool**, specify whether to use the default sensor pool or to be provided a list of sensor pools to choose from when you start a Fortify ScanCentral SAST scan.

   Note: If Fortify ScanCentral SAST has SSC lockdown mode enabled, Fortify ScanCentral SAST automatically uses either the sensor pool associated with a selected application version or the default sensor pool.
9. (Optional) In the **Notification Email** box, type an email address for job status notification.
10. Click **OK** to save your configuration.

Scanning Projects with ScanCentral SAST

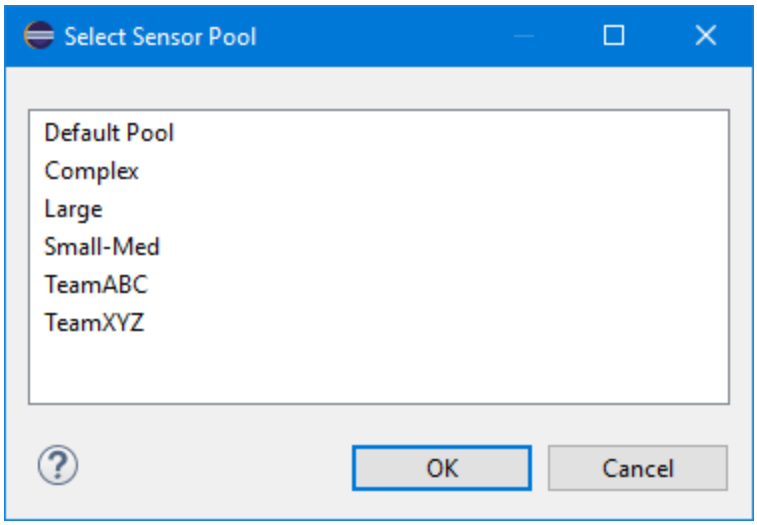
Before you can scan your project with Fortify ScanCentral SAST, you must configure the Fortify ScanCentral SAST analysis options as described in "Configuring Fortify ScanCentral SAST Options" on page 35.

Note: To scan projects that have special translation or build conditions or have files you want to exclude from the project, use the advanced analysis (see "Running an Advanced Analysis" on the next page).

To scan a project with Fortify ScanCentral SAST:

1. In the **Package Explorer** or **Project Explorer** view, select a project.
2. Start the scan by doing one of the following:
   - To perform a remote translation and remote scan, select **Fortify > Analyze Project with ScanCentral > Remote Translation**.
   - To perform a local translation and remote scan, select **Fortify > Analyze Project with ScanCentral > Local Translation**.
3. If prompted, select the application version where you want to upload the analysis results, and then click **OK**.
4. If prompted, select a sensor pool, and then click **OK**.

Note: If Fortify ScanCentral SAST is in SSC lockdown mode, then you must select the default sensor pool.



To view the analysis results, you can either:

- Copy the provided job token and use it in the Fortify ScanCentral SAST command-line interface to check the status and retrieve the analysis results (see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*). You can then open the analysis results in Eclipse (see "Opening an Audit Project" on page 105).

  Tip: If you need to retrieve the job token, you can find it in the Fortify ScanCentral SAST log file. The default log file locations are listed in "Locating Log Files" on page 127.

- If you uploaded the analysis results to Fortify Software Security Center, you can check the status of the job (and view the results) on the Fortify Software Security Center server. After the scan is complete, you can open the results in Eclipse using the Fortify Remediation Plugin for Eclipse.

Running an Advanced Analysis

Use advanced analysis to scan 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.

Before you use advanced analysis with Fortify ScanCentral SAST, make sure you configure the Fortify ScanCentral SAST options (see "Configuring Fortify ScanCentral SAST Options" on page 35) and you have a properly configured Fortify ScanCentral SAST installation. For more information, see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

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

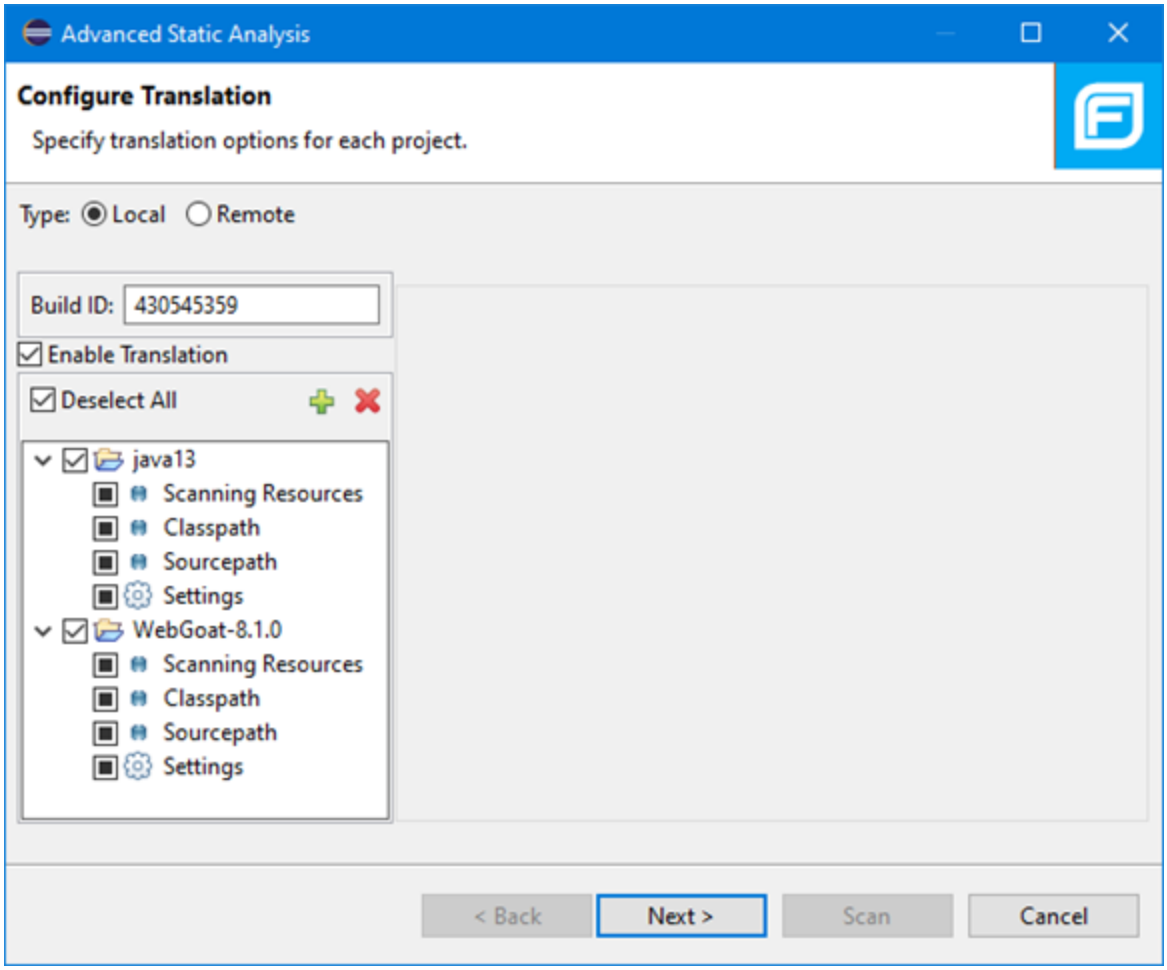
To perform an advanced analysis:

1. From Eclipse, select one or more projects.

   Note: If no projects are selected, then the advanced analysis wizard includes all projects. You can remove projects from advanced analysis as necessary in the wizard (see the following step).

2. Select **Fortify > Advanced Analysis**.

   The Advanced Static Analysis wizard opens.



   The selected Eclipse projects to be scanned are listed in the left pane. To exclude a project from the advanced analysis, clear the check box for the project.

3. Under **Type**, specify where you want to run the translation phase of the analysis. Do one of the following:

   - To run the translation phase using a locally installed instance of Fortify Static Code Analyzer, select **Local**.

     On the next page in the wizard, you can select whether to run the scan phase locally or remotely with Fortify ScanCentral SAST.

   - To run the entire analysis with Fortify ScanCentral SAST, select **Remote**.

When Fortify ScanCentral SAST performs the translation phase, it will automatically run the scan phase as well.

4. In the Build ID box, type the build ID.

   If you selected only one project for the advanced analysis, the root directory name is the default build ID. Otherwise, the wizard creates a unique number for the build ID, which you can change.

5. 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 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.

6. 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 folders for translation, click the **Add Folders** button.

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

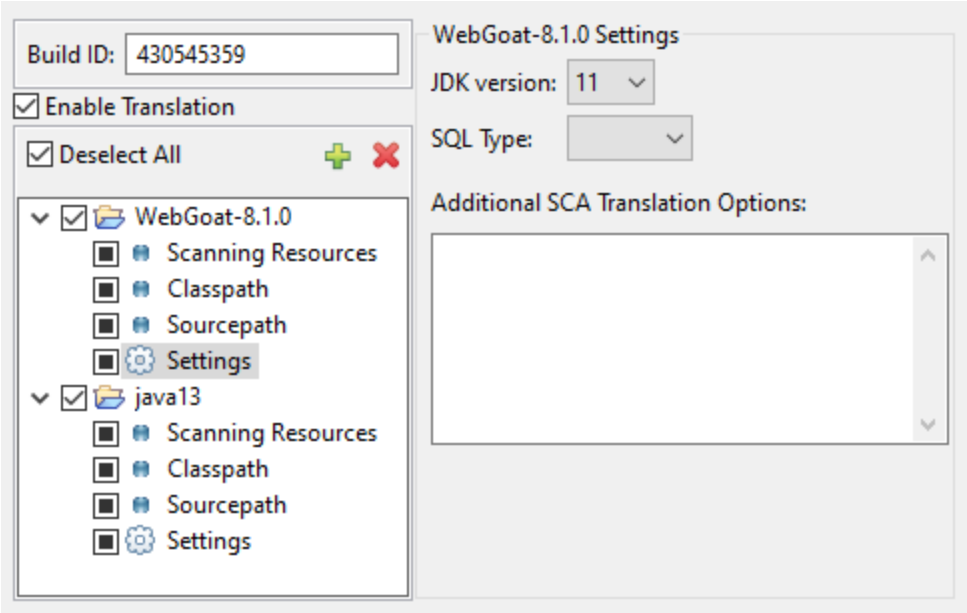
     Make sure to select only the files or directories that you want to translate. To add additional files for translation, click the **Add Folders** button. To add JAR files, click the **Add JAR** button.

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

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

7. Click **Settings** for each Eclipse project to specify additional Fortify Static Code Analyzer translation options.

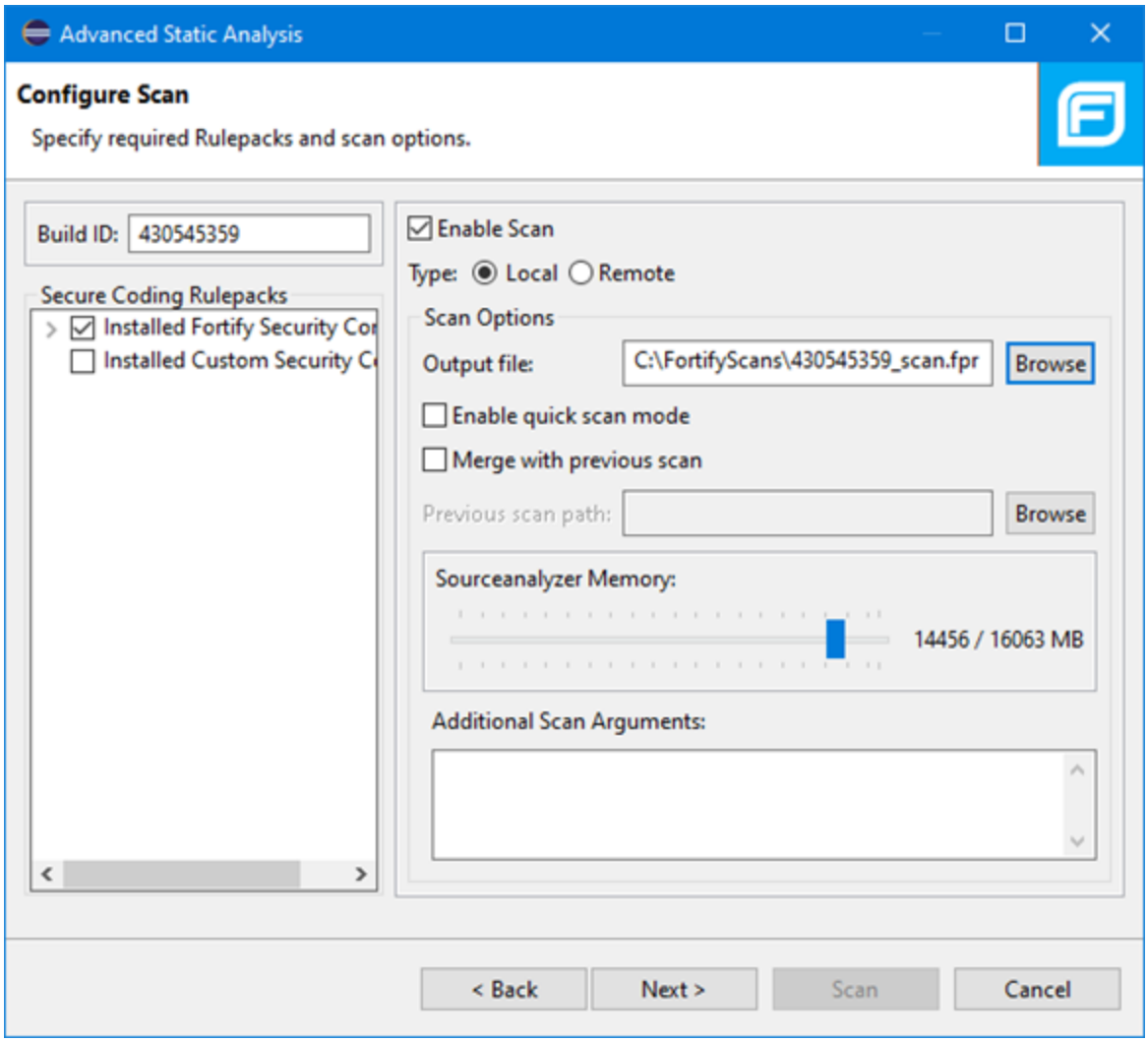
   Note: The translation setting options available depend on the Eclipse project type. The following image shows the options for a Java project.



a. From the **JDK version** list, select the Java version of the code in the project.
b. By default, Fortify Static Code Analyzer treats SQL files as T-SQL on Windows (and Linux for .NET projects only). To specify the SQL type, from the **SQL Type** list, select **TSQL** or **PLSQL**.
c. Specify any additional translation options in the **Additional SCA Translation Options** box.

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

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



9. For **Type**, select where to run the scan phase of the analysis by selecting one of the following:
   - **Local**—Run the scan phase on the local system. You can adjust any of the following scan options for a local scan:
     i. To skip the scan phase, clear the **Enable Scan** check box.

        For example, to offload the scan phase to a different machine, 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 *OpenText™ Fortify Static Code Analyzer User Guide* for instructions on how to use mobile build sessions.

     ii. 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.

     iii. To perform a quick scan, select the **Enable quick scan mode** check box.

        For information about quick scans, see "About Quick Scan Mode" on page 28.

     iv. 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.

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

Note: The Fortify Plugin for Eclipse displays the amount of memory specified for Fortify Static Code Analyzer followed by the amount of memory on your system.

- **Remote**—Run the scan phase with Fortify ScanCentral SAST.

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

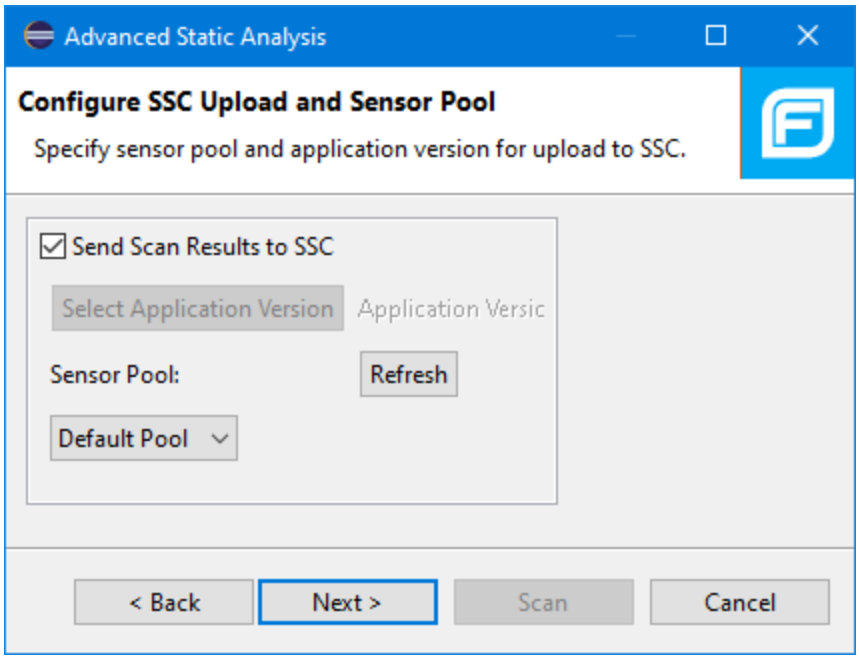
    For information about the available Fortify Static Code Analyzer command-line scan options, see the *OpenText™ Fortify Static Code Analyzer User Guide*.

11. (Optional) To scan the code with a custom selection of Fortify Secure Coding Rulepacks, do the following:
    a. In the **Secure Coding Rulepacks** list in the left pane, 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 23.

12. Click **Next**.

    (Remote analysis only) The Configure SSC Upload and Sensor Pool page displays options to upload the analysis results to Fortify Software Security Center and to select the sensor pool.



    a. To upload the analysis results to Fortify Software Security Center:
        i. Select **Send Scan Results to SSC**.
        ii. Click **Select Application Version**.

iii. In the Choose Application and Version Mapping for Upload results dialog box, select an application version.

iv. Click **OK**.

b. (Optional) Select a sensor pool from the **Sensor Pool** list, and then click **Next**.

The default sensor pool is selected by default.

Note: If Fortify ScanCentral SAST has SSC lockdown mode enabled, then you must select the default sensor pool.

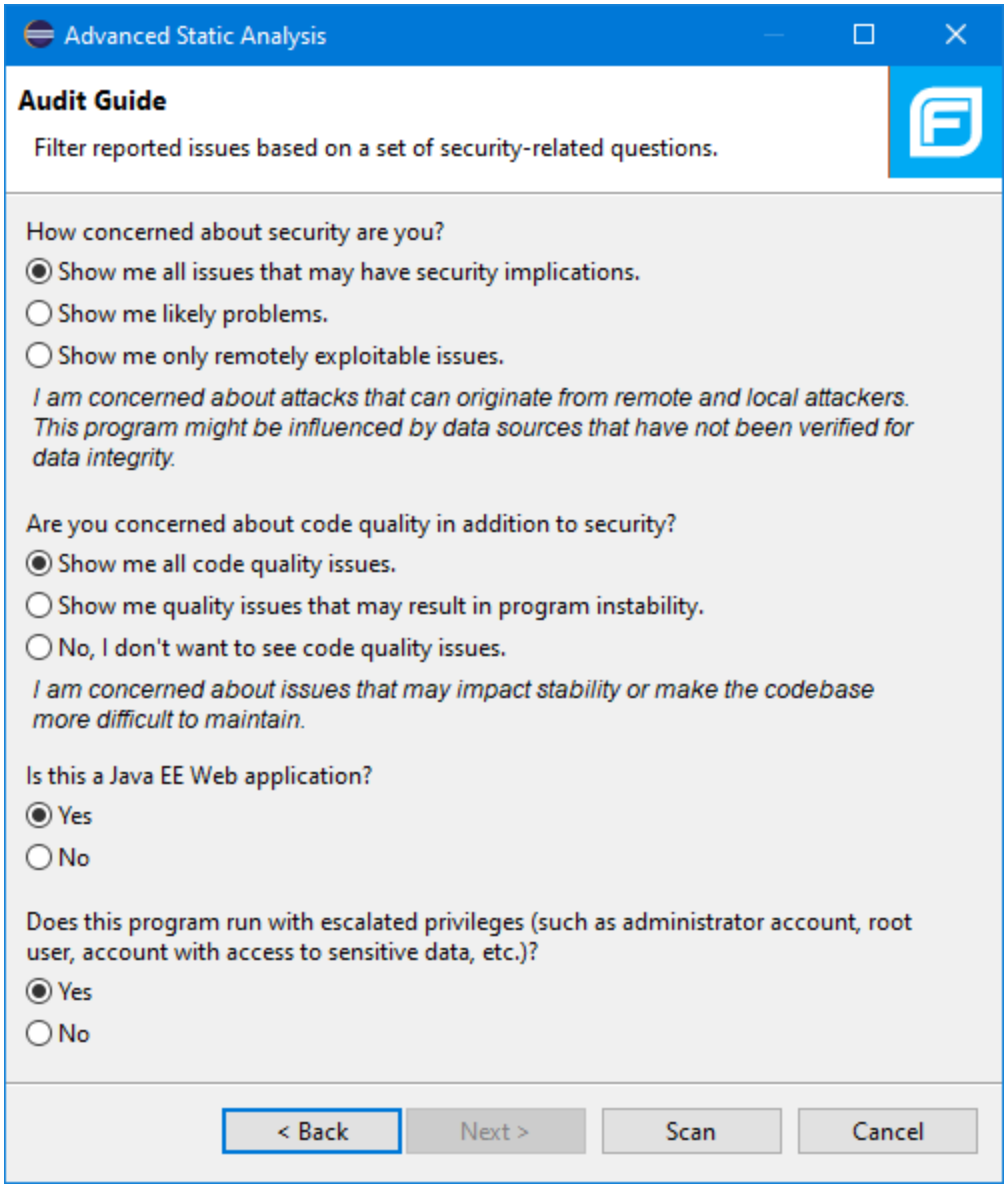
Note: You can click **Refresh** to update the sensor pool list if necessary.

The Preview SCA Commands page displays a preview of the Fortify Static Code Analyzer or Fortify ScanCentral SAST commands to be used for the analysis.

13. (Optional) On the Preview SCA Commands page, you can review and change the Fortify Static Code Analyzer translation and scan commands.

Note: You cannot edit a Fortify ScanCentral SAST command.

14. For a local analysis only, click **Next** to proceed to the Audit guide page, where you can select additional scan settings.



15. Click **Scan** to run the analysis.

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

For a local analysis (both translation and scan), after the scan completes successfully, the analysis results are displayed in the Fortify Audit perspective.

To view the analysis results from a Fortify ScanCentral SAST analysis, do one of the following:

- Copy the provided job token and use it in the Fortify ScanCentral SAST command-line interface to check the status and retrieve the analysis results (see the *OpenText™ Fortify ScanCentral SAST*

Installation, Configuration, and Usage Guide). You can then open the analysis results in Eclipse (see "Opening an Audit Project" on page 105).

Tip: If you need to retrieve the job token, you can find it in the Fortify ScanCentral SAST log file. The default log file locations are listed in "Locating Log Files" on page 127.

- If you uploaded the analysis results to Fortify Software Security Center, you can check the status of the job (and view the results) on the Fortify Software Security Center server. After the scan is complete, you can open the results in Eclipse using the Fortify Remediation Plugin for Eclipse.

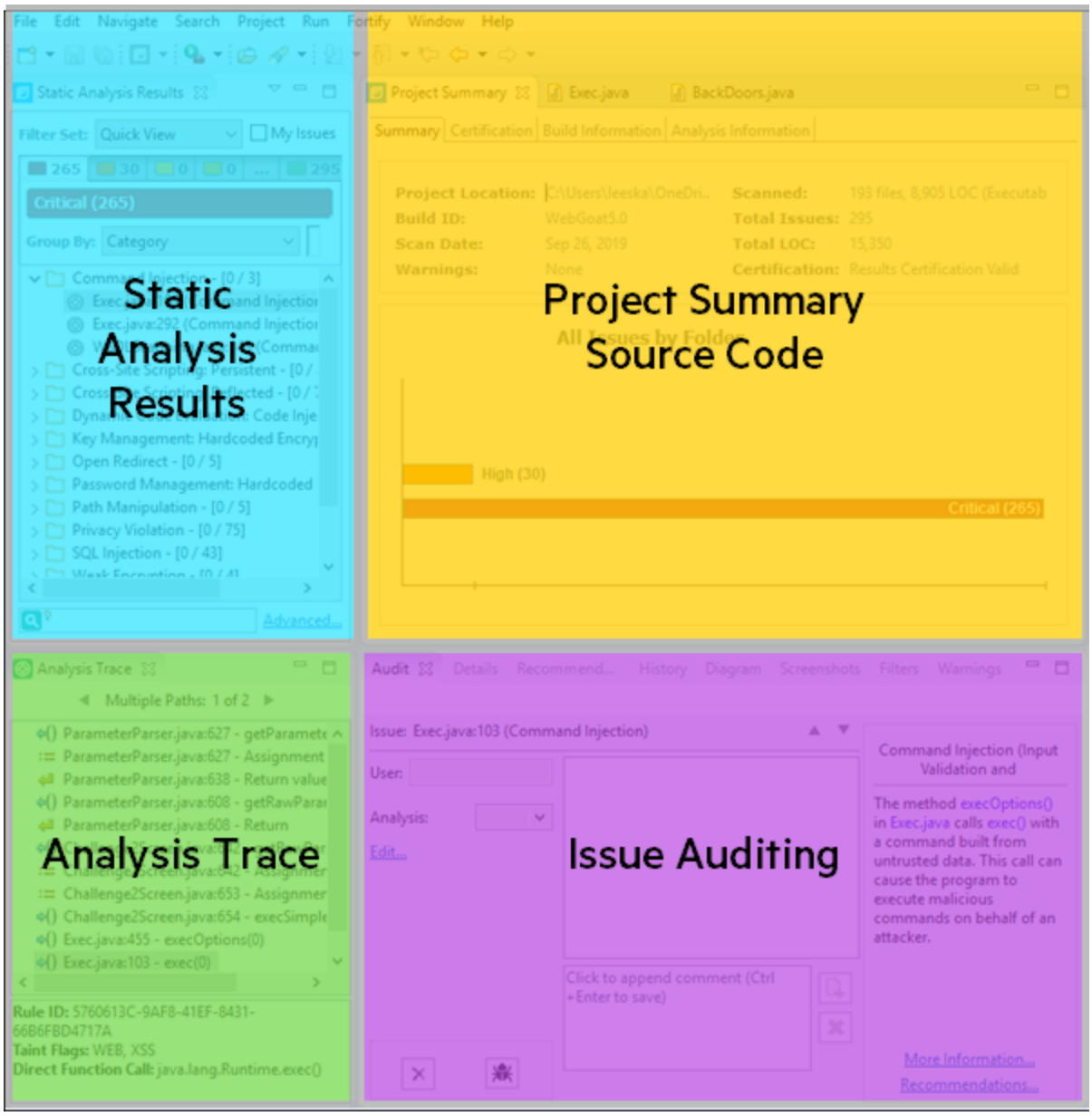
Chapter 4: Viewing Analysis Results

After a scan is completed, the Fortify Plugin for Eclipse displays the analysis results in the Fortify Audit perspective.

This section contains the following topics:

About Viewing Analysis Results

The Fortify Audit perspective displays four audit-focused views. After the scan is complete (or, after you open an existing audit project), summary analysis 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.



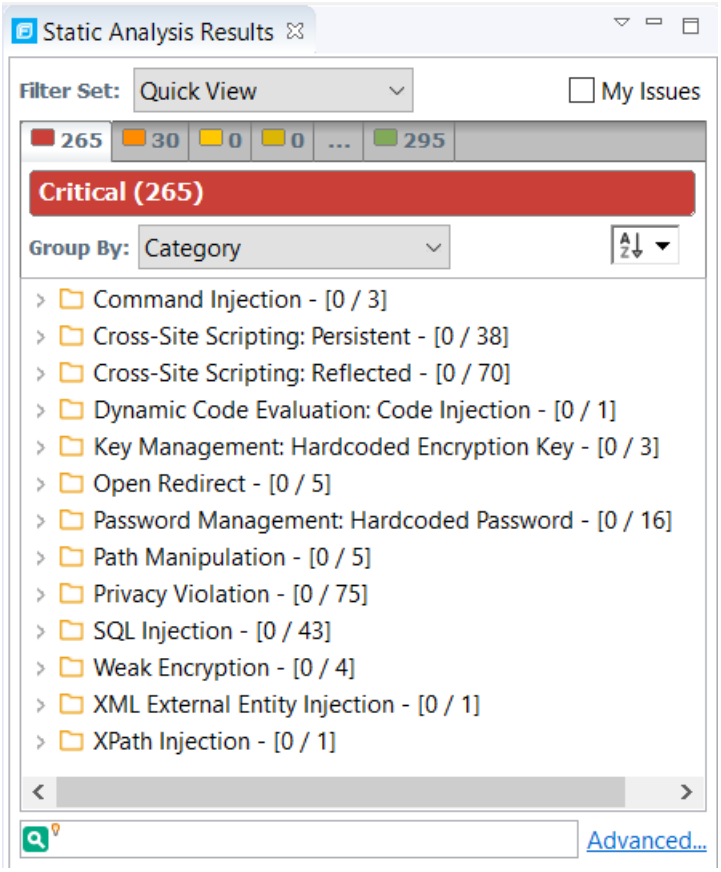
View / Tab	More Information
Static Analysis Results (top left)	"Static Analysis Results View" below
Project Summary (top center)	"Project Summary View" on page 54
Analysis Trace (bottom left)	"Analysis Trace View" on page 59
Issue Auditing (bottom center)	"Issue Auditing View" on page 61

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 lists the issues detected in the application and provides several ways to group them. 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 82.

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 turn off the default filter set so that the Fortify Eclipse Complete Plugin uses the filter set last enabled in the issue template to display analysis results for new projects.

To select the filter set for new or opened projects:

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

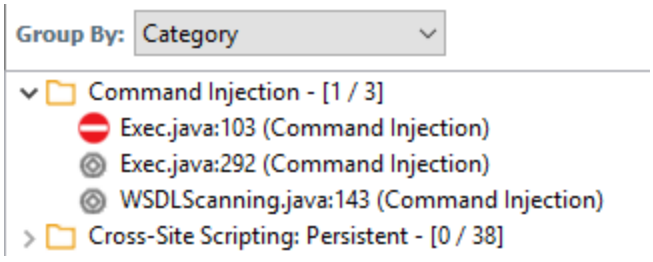
   If you clear the check box, the default filter is loaded. For newly-opened projects, the default filter for FPRs that have no embedded template or the default filter from the embedded template is the Security Auditor View filter set.
4. From the list to the right of the **Default Filter Set** check box, select the filter set to use to display analysis 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 Fortify Eclipse Complete Plugin, the term folder *does not* refer to the folder in the issues list.

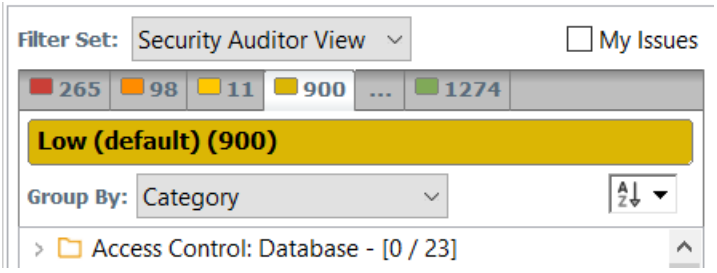
Within each color-coded folder, issues are grouped into subfolders. At the end of each folder name, enclosed in brackets, is the number of audited issues and the total number of issues in the folder. For example, **Command Injection - [1 / 3]** indicates that one out of three issues categorized as Command Injection has been audited.



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

Folder	Description
Critical	This 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.
High	This 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.
Medium	This folder contains issues that have a 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.
Low	This folder contains issues that have a low impact and a low likelihood of exploitation. 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. Remediate these issues as time permits.
All	This folder contains all the issues.

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 87.

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 68).

Group By List

You can use the **Group By** list of grouping attributes to sort the issues into subfolders. The grouping attribute 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 grouping attributes apply to the application instance. You can apply the grouping attributes to any project opened with that instance of the application.

See Also

"Grouping Issues" on page 98

"Creating a Custom Grouping Option" on page 101

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 pane, select **Audit Configuration**, and then select 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	Button	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

Sort Method	Button	Description
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 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

Use the search box 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 "Search Syntax" on page 71.

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.

Note: If the **Summary** tab header indicates that there are warnings in your scan, you can review them in more detail in the Issue Auditing view. For more information, see "Warnings Tab" on page 66.

Certification Tab

The **Certification** tab displays the certification status for the analysis results. Results certification is a check to ensure that the analysis results were not altered after Fortify Static Code Analyzer produced them

Build Information Tab

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

- Build details including the build ID, build label, 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
- Total lines of code (Total LOC) scanned

  The total number of lines of code, including blank lines and comments
- List of files scanned with file sizes and timestamps
- Libraries referenced in the scan
- Java class path used in the translation

Analysis Information Tab

The **Analysis Information** tab shows the version of Fortify Static Code Analyzer 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 configuration properties used in the scan
- **Commandline Arguments**—Displays the command-line options used to scan the project

Viewing Summary Graph Information

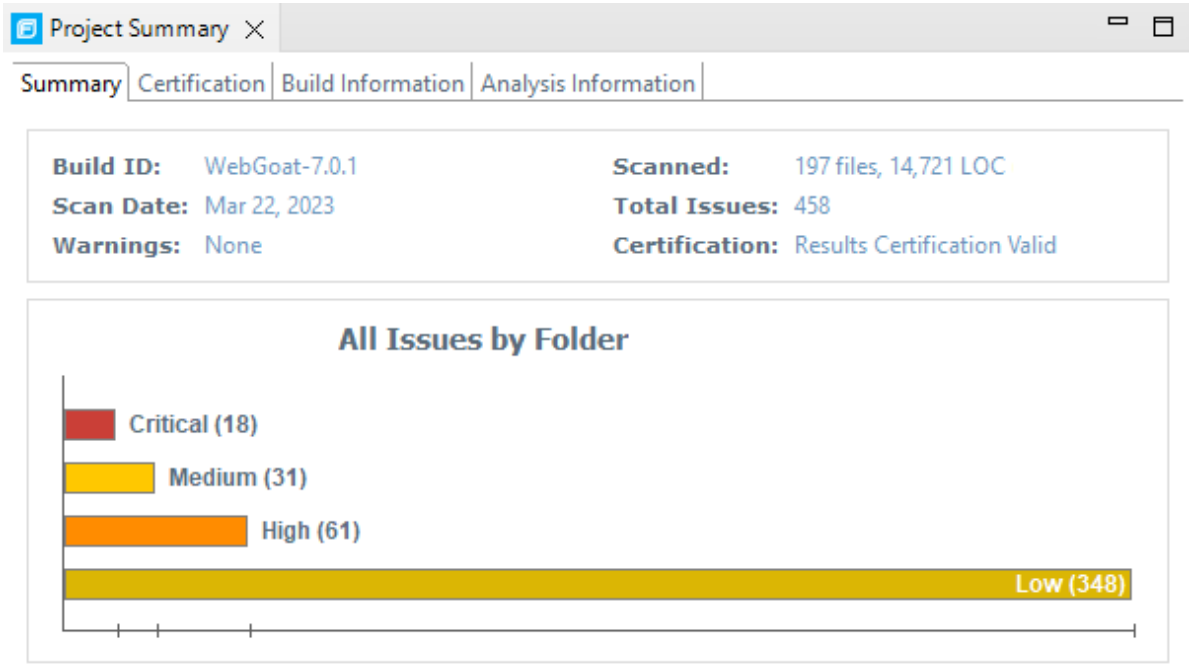
The summary graph displayed in the **Project Summary** view provides multiple perspectives on the sets of issues, grouped by priority (Critical, High, Medium, and Low) uncovered in a scan. You can drill down in the graph to see detailed information about each issue set, and create various bar charts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

To access details about issue sets in an audit project:

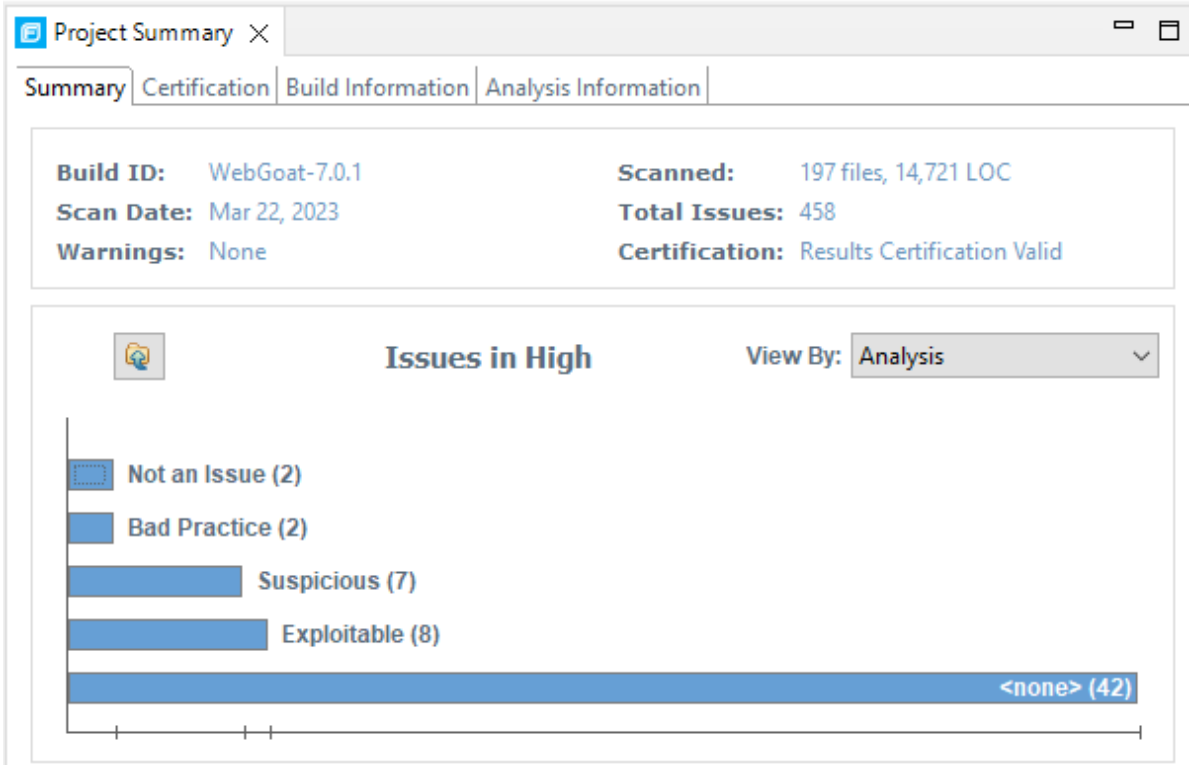
1. Scan your project source code or open an existing audit project.

   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.



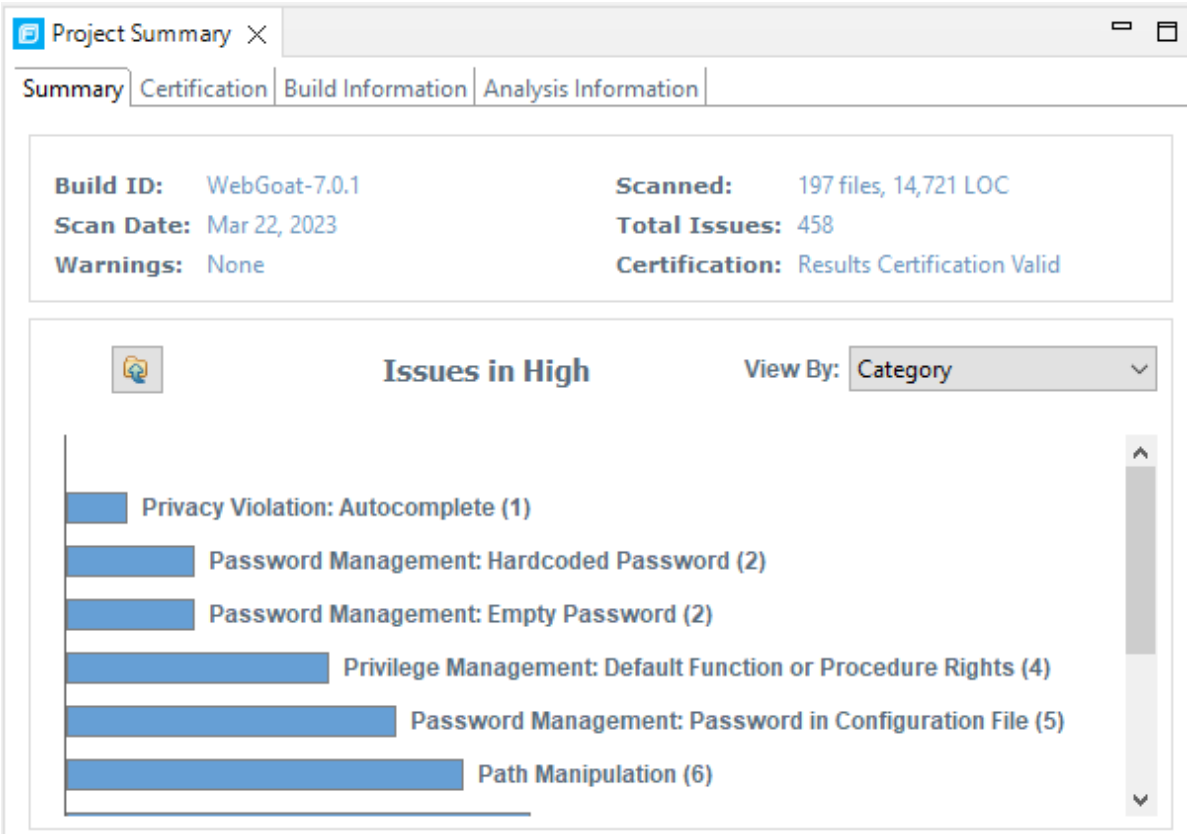
2. To see a different view of the high priority issues, click the **High** bar.



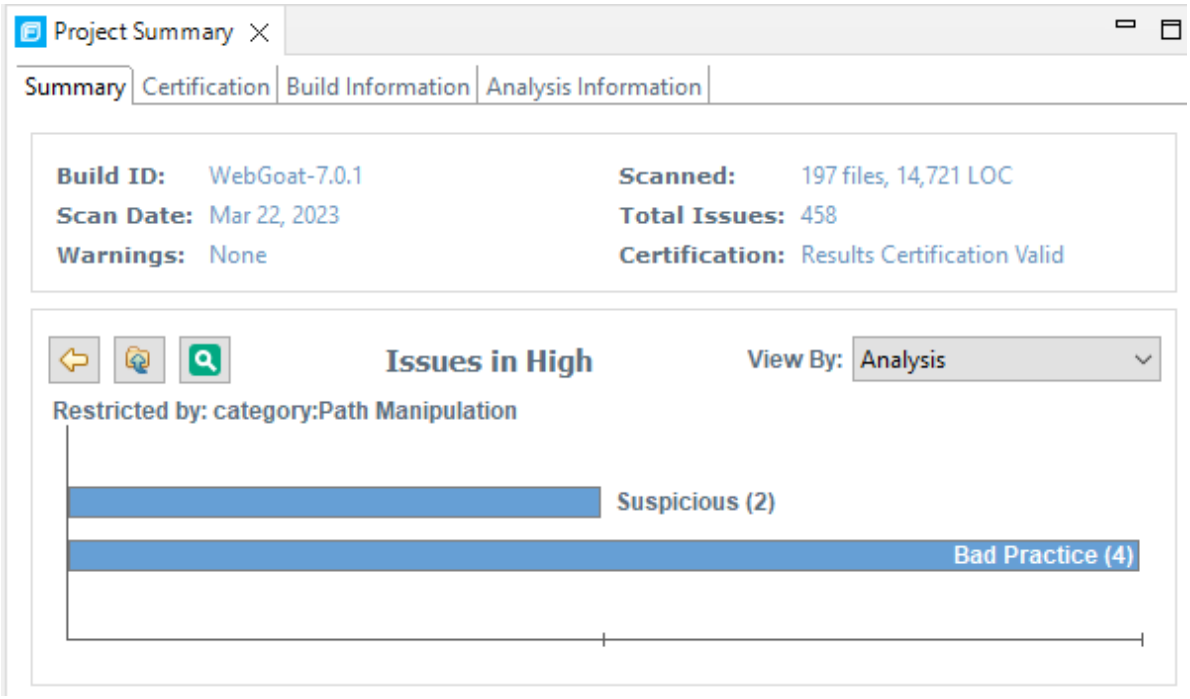
By default, the graph displays high priority issues based on the analysis attribute (assigned analysis values).

Note: The example here shows information for analysis 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.

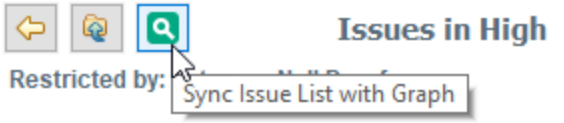


4. On the **Issues in High** bar graph, select a bar for a category that contains multiple issues.

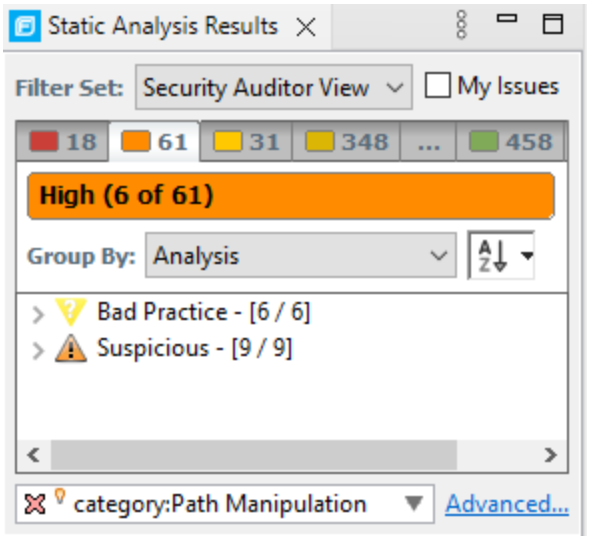


In the example shown here, the **Path Manipulation** bar is selected. You can see that of the six issues, two are marked as Suspicious and four are marked as Bad Practice.

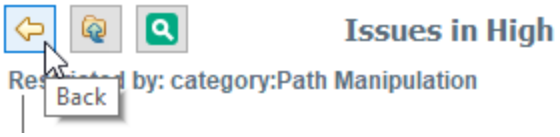
5. To synchronize the issues list with the displayed graphical view, click the **Sync Issue List with Graph** button.



The issue 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 the **Back** button.



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

Analysis Trace View

When you select an issue, the **Analysis Trace** view displays the relevant analysis trace. This is a set of program points that show how the analyzer found the issue. For dataflow and control flow issues, the set is presented in the order executed. For dataflow issues, this trace view presents the path that the tainted data follows from the source function to the sink function.

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

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 symbols described in the following table to show how the dataflow moves in this section of the source code or execution order.

Symbol	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 web address
	Data is assigned to a globally scoped field or variable
	A comparison is made
	The function call receives tainted data
	The function call returns tainted data
	Passthrough, tainted data passes from one place to another **Note:** This is typically shown as `functionA(x : y)` to indicate that data is transferred from `x` to `y`. The `x` and `y` values are one of the following: • An argument index • `return`—The return value of a function • `this`—The instance of the current object • A specific object field or key
	An alias is created for a memory location
	Data is read from a variable
	Data is read from a global variable
	Tainted data is returned from a function
	A pointer is created
	A pointer is dereferenced
	The scope of a variable ends

Symbol	Description
	The execution jumps
	A branch is taken in the code execution
	A branch is not taken in the code execution
	Generic
	A runtime source, sink, or validation step
	Taint change

The **Analysis Trace** view can include inductions. Inductions provide supporting evidence for their parent nodes. Inductions consist of:

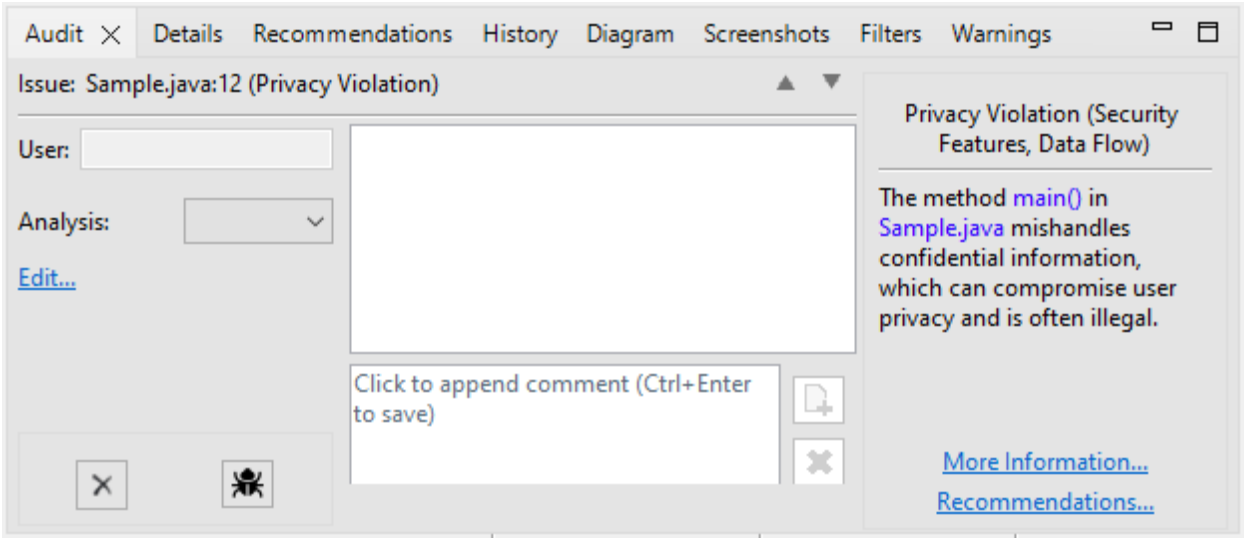
- A text node, displayed in italics as a child of the trace node. This text node is expanded by default.
- An induction trace, displayed as a child of the text node (a box surrounds the induction trace).

The italics and the box distinguish the induction from a standard subtrace. To display the induction reference information for that induction, click it.

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, which are 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 interface 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 Fortify Software Security Center and a user was assigned.
Analysis	Displays the audit assessment for the selected issue. To change the assessment, select an item from the list. This is the primary tag. The default primary tag is **Analysis**, but it might be different depending on the custom tag settings in the project configuration. The valid values for **Analysis** are Not an Issue, Reliability Issue, Bad Practice, Suspicious, and Exploitable.
<custom_tagname>	Displays any custom tags if defined for the audit project. These are displayed below the primary tag. If the audit results were submitted to OpenText™ Fortify Audit Assistant in Fortify Software Security Center, then in addition to any other custom tags, the tab displays the following tags: • **AA_Prediction**—Exploitability level that Fortify Audit Assistant assigned to the issue. You cannot modify this tag value. • **AA_Confidence**—Confidence level from Fortify Audit Assistant for the accuracy of its **AA_Prediction** value. You cannot modify this tag value. • **AA_Training**—Whether to include or exclude the issue from Fortify Audit Assistant training. You can modify this value. For more information about Fortify Audit Assistant, see the *OpenText™ Fortify Software Security Center User Guide*.
	Suppresses the issue.
	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**.

Element	Description
	Provides access to a supported bug tracker.
Comment	Appends additional information about the issue to the comment box.
Rule Information	Shows information, such as the category and kingdom that describes the issue.
More Information	Opens the **Details** tab (see "Details Tab" below).
Recommendations	Opens the **Recommendations** tab (see "Recommendations Tab" on the next page).
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 an abstract of the issue, a detailed explanation, and examples. The following table describes the tab sections.

Section	Description
Abstract/Custom Abstract	Summary of the issue, including any custom abstracts defined by your organization.
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 section also includes any custom explanations defined by your organization.
Instance ID	Unique identifier for the issue.
Priority Metadata Values	Priority metadata values for this issue including impact and likelihood.
Legacy Priority Metadata Values	Legacy priority metadata values for the issue including severity and confidence.

WebInspect Agent Details Tab

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

Section	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 describes the tab sections.

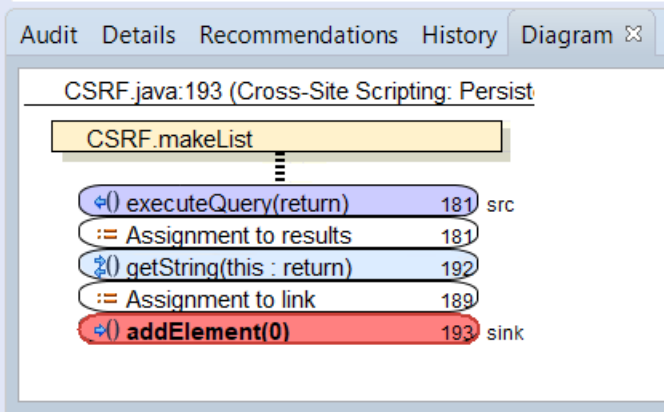
Section	Description
Recommendations/Custom Recommendations	Describes possible solutions for the selected issue. It can also include examples and recommendations defined by your organization.
Tips/Custom Tips	Provides useful information specific to the selected issue, and any custom tips defined by your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

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.



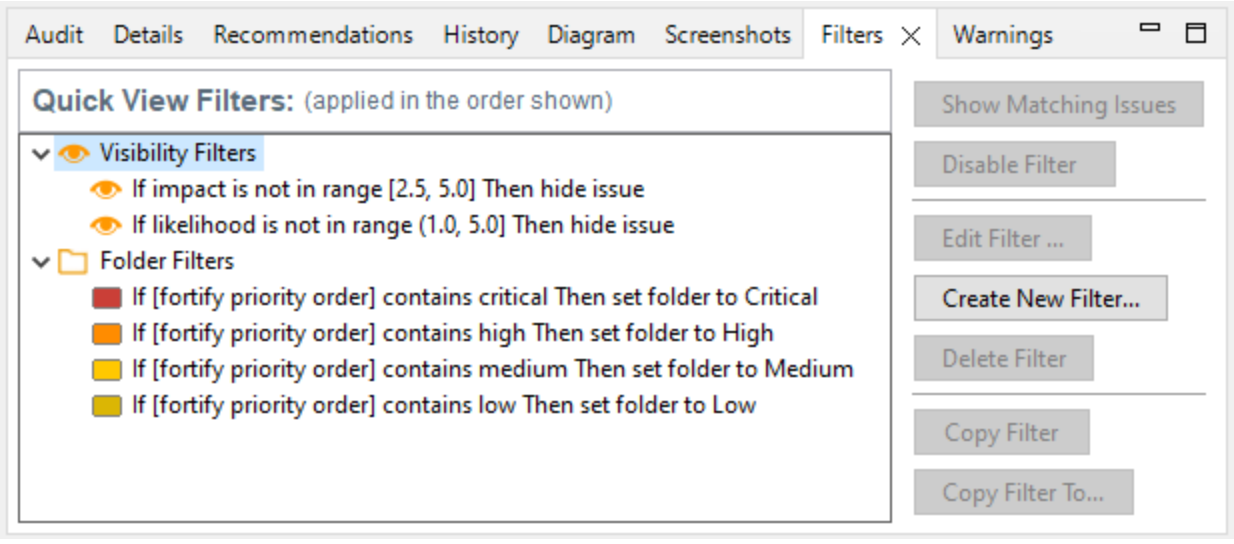
For dataflow issues, the trace starts with the first function to call the taint source, then traces the calls to the source (blue node) and ends the trace at the sink (red node). In the diagram, the source (src) and sink nodes are also labeled. A red X on a vertical axis indicates that the called function 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 symbols used for the expression type of each node in the diagram are the same symbols used in the **Analysis Trace** view. For a description of the symbols, see "Analysis Trace View" on page 59.

Filters Tab

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



The following table describes the options to create new filters.

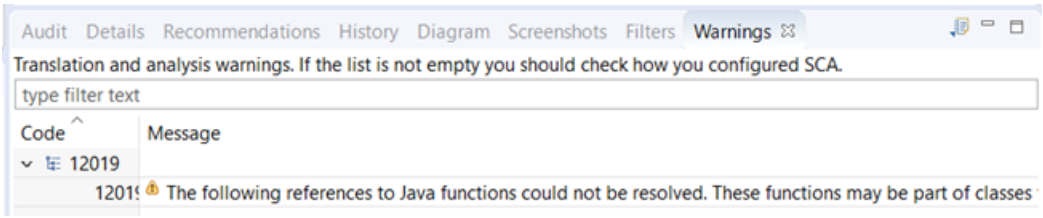
Option	Description
Filters	Displays a list of the visibility and folder filters configured in the selected filter set where: • Visibility filters show or hide issues • Folder filters sort the issues into the folder tabs in the Static Analysis Results view Right-click a filter to show issues that match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

See Also

"Creating a Filter from the Issue Auditing View" on page 83.

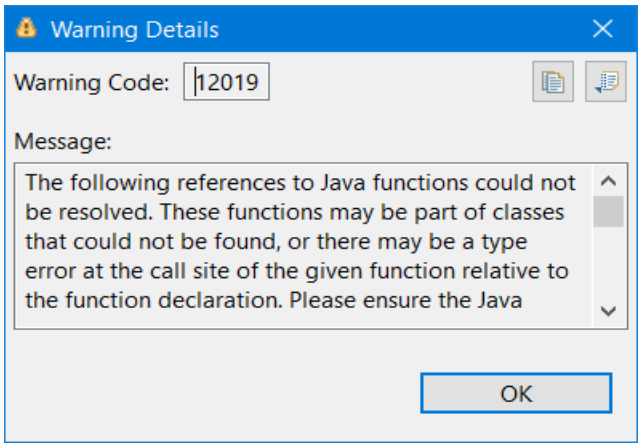
Warnings Tab

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 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 the **Export Warnings** button  . 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: `<userhome>/.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.

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 pane, 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 (off by default).
Show Removed Issues	Displays all issues detected in the previous scan, 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. Fortify Static Code

Preference	Description
	Analyzer marks these vulnerabilities as Removed Issues.
Show Hidden Issues	Displays all hidden issues.
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**.

Searching for Issues

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

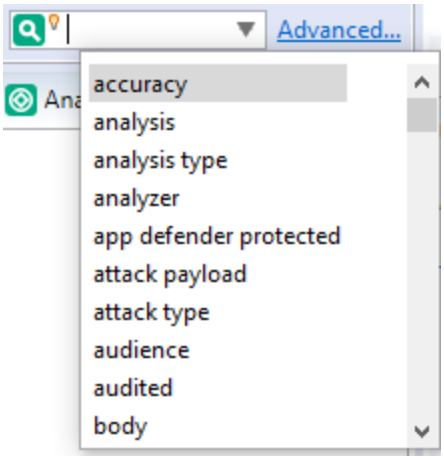
To perform a simple search, do one of the following:

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

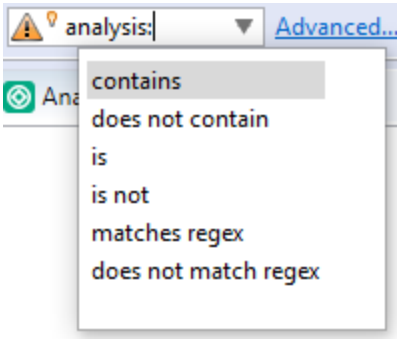
- To select a search query that you used before, click the arrow in the search box, and then select a search query from the list.

To get assistance with composing a search query, do the following:

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



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



4. From the displayed list, double-click a comparison to add it to your search query.
5. Type the rest of the search query, and then press **Enter** to perform the search.

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

Creating complex search strings can involve several steps. If you type an invalid search query, the magnifying glass in the search box changes to a warning to notify you of the error. Click the warning sign to view information about the search query 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" on page 79.

See Also

"Search Syntax" below

"Search Modifiers" on the next page

"Search Query Examples" on page 79

"Performing Advanced Searches" on page 79

Search Syntax

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

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

You can further qualify search terms with modifiers. The syntax for using a modifier is *<modifier>:<search_term>*.

A search query can contain multiple modifiers and search terms. If you specify more than one modifier, the search returns only issues that match all the modified search terms. For example,

`file:ApplicationContext.java category:SQL Injection` returns only SQL injection issues found in `ApplicationContext.java`.

If you use the same modifier more than once in a search query, then the search terms qualified by those modifiers are treated as an `OR` comparison. For example, `file:ApplicationContext.java category:SQL Injection category:Cross-Site Scripting` returns SQL injection issues and cross-site scripting issues found in `ApplicationContext.java`.

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

See Also

"Search Modifiers" below

"Search Query Examples" on page 79

"Searching for Issues" on page 70

"Performing Advanced Searches" on page 79

Search Modifiers

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

A search that is not qualified by a modifier matches the search query based on the following attributes: kingdom, primary rule id, analyzer, filename, severity, class name, function name, instance id, package, confidence, type, subtype, taint flags, category, sink, and source.

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

- To apply the search to all modifiers, type a string such as `control flow`. This searches all the modifiers and returns any results that contain the "control flow" string.
- To apply the search to a specific modifier, type the modifier name and the string as follows: `analyzer:control flow`. This returns all results detected by the Control Flow Analyzer.

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

Search Modifier (Issue Attribute)	Description
`accuracy`	Searches for issues based on the accuracy value specified (0.1 through 5.0).
`analysis`	Searches for issues that have the specified audit analysis value such as `exploitable`, `not an issue`, and so on.

Search Modifier (Issue Attribute)	Description
`[analysis type]`	Searches for issues based on the analyzer product such as `SCA` and `WEBINSPECT`.
`analyzer`	Searches the issues for the specified analyzer such as `control flow`, `data flow`, `structural`, and so on.
`[app defender protected]` (`def`)	Searches for issues based on whether Application Defender can protect the vulnerability category (`protected` or `not protected`).
`[attack payload]`	Searches for issues that contain the search term in the part of the request that caused the vulnerability for penetration test results.
`[attack type]`	Searches for issues based on the type of penetration test attack conducted (URL, parameter, header, or cookie).
`audience`	Searches for issues based on intended audience such as `dev`, `targeted`, `medium`, `broad`, and so on. **Note:** This metadata is legacy information that is no longer used and will be removed in a future release. OpenText recommends that you do not use this search modifier.
`audited`	Searches the issues to find `true` if the primary tag is set and `false` if the primary tag is not set. The default primary tag is the Analysis tag.
`body`	Searches for issues that contain the search term in the HTTP message body in penetration test results, which is all the data that is transmitted immediately following the headers.
`bug`	Searches for issues that contain the search term in the information for the filed bug. **Note:** This information is discarded each time you restart Eclipse.
`category` (`cat`)	Searches for the specified category or category substring.

Search Modifier (Issue Attribute)	Description
`class`	Searches for issues based on the specified class name.
`codesnippet`	Searches for the specified string within the few lines of code that are stored for each vulnerability by default. If code snippets were excluded from the scan results during the analysis, then the search will not return any results.
`comments` (`comment`, `com`)	Searches for issues that contain the search term in the comments added to the issue.
`commentuser`	Searches for issues with comments from a specified user.
`confidence` (`con`)	Searches for issues that have the specified confidence value 0.1 through 5.0 (legacy metadata).
`cookies`	Searches for issues that contain the search term in the cookie from the HTTP query for penetration test results.
`correlated`	Searches for issues based on whether the issues are correlated with another analyzer.
`[correlation group]`	Searches for issues based on whether the issues are in the same correlation group.
<custom_tagname>	Searches for issues based on the value of the specified custom tag. You can search a list-type custom tag using a range of values. The values of a list-type custom tag are an enumerated list where the first value is 0, the second is 1, and so on. You can use the search syntax for a range of numbers to search for ranges of list-type custom tag values. For example, `analysis:[0,2]` returns the issues that have the values of the first three analysis values, 0, 1, and 2 (Not an Issue, Reliability Issue, and Bad Practice). To search for a specific date in a date-type custom tag, specify the date in the format: yyyy-mm-dd. To search for issues that have no value set for a custom tag, use `<none>` for the search term. For example, to search for all issues that have no value set in the custom tag labeled Target

Search Modifier (Issue Attribute)	Description
	Date, type: `[Target Date]:<none>`.
`dynamic`	Searches for issues that have the specified dynamic hot spot ranking value.
`[engine priority]`	Searches for issues based on the original priority value determined by the engine that identified the issue.
`file`	Searches for issues where the primary location or sink node function call occurs in the specified file path.
`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 issue priority. Valid values are `critical`, `high`, `medium`, and `low`.
`headers`	Searches for issues that contain the search term in the request header for penetration test results.
`historyuser`	Searches for issues that have audit data modified by the specified user.
`[http version]`	Searches for issues based on the specified HTTP version such as `HTTP/1.1`.
`impact`	Searches for issues based on the impact value specified (0.1 through 5.0).
`[instance id]`	Searches for an issue based on the specified instance ID.
`[issue age]`	Searches for the issue age, which is `new`, `updated`, `reintroduced`, or `removed`.
`[issue state]`	Searches for audited issues based on whether the issue is an open issue or not an issue (determined by the level of analysis set for the primary tag).
`kingdom`	Searches for all issues in the specified kingdom.
`likelihood`	Searches for issues based on the specified likelihood value (0.1

Search Modifier (Issue Attribute)	Description
	through 5.0).
`line`	Searches for issues on the primary location line number. For dataflow issues, the value is the sink line number. See also "sourceline" on page 78.
`manual`	Searches for issues that were manually created by penetration test tools, and not automatically produced by a web crawler such as OpenText™ Fortify WebInspect.
`[mapped category]`	Searches for issues based on the specified category that is mapped across the various analyzers (Fortify Static Code Analyzer, Fortify WebInspect, and Fortify WebInspect Agent).
`maxconf`	Searches for all issues that have a confidence value equal to or less than the number specified as the search term.
`maxVirtConf`	Searches for dataflow issues that have a virtual call confidence value equal to or less than the number specified as the search term.
<metadata_listname>	Searches for issues based on the value of the specified metadata external list. Metadata external lists include `[owasp top ten <year>]`, `[cwe top 25 <version>]`, `[pci ssf <version>]`, `[stig <version>]`, and others.
`method`	Searches for issues based on the method, such as `GET`, `POST`, `DELETE`, and so on.
`minconf`	Searches for all issues that have a confidence value equal to or greater than the number specified as the search term.
`min_virtual_call_confidence` (`virtconf`, `minVirtConf`)	Searches for dataflow issues that have a virtual call confidence value equal to or greater than the number specified as the search term.
`package`	Searches for issues where the primary location occurs in the specified package or namespace. For dataflow issues, the primary location is the sink function.
`parameters`	Searches for issues that contain the search term in the HTTP

Search Modifier (Issue Attribute)	Description
	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. See also "sink" below and "[source context]" below.
`primaryrule (rule)`	Searches for all issues related to the specified sink rule.
`probability`	Searches for issues based on the probability value specified (1.0 through 5.0).
`[remediation effort]`	Searches for issues based on the remediation effort value specified. The valid values are whole numbers from 1.0 to 12.0.
`[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.
`severity (sev)`	Searches for issues based on the specified severity value (legacy metadata).
`shortfilename`	Searches for issues where the primary location or sink node function call occurs in file names that contain the specified search term, but not anywhere in its full path. For full path matches, use the modifier "file" on page 75.
`sink`	Searches for issues that have the specified sink function name. See also "[primary context]" above.
`source`	Searches for dataflow issues that have the specified source function name. See also "[source context]" below.
`[source context]`	Searches for dataflow issues that have the source function call

Search Modifier (Issue Attribute)	Description
	contained in the specified code context. See also "source" on the previous page and "[primary context]" on the previous page.
`sourcefile`	Searches for dataflow issues with the source function call that the specified file contains. See also "file" on page 75.
`sourceline`	Searches for dataflow issues having taint source entering the flow on the specified line. See also "line" on page 76.
`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.
`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.
`tracenodeAllPaths`	Searches for the specified value in all the steps of analysis trace.
`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 web address.
`user`	Searches for issues assigned to the specified user.

Search Query Examples

The following table contains search query examples.

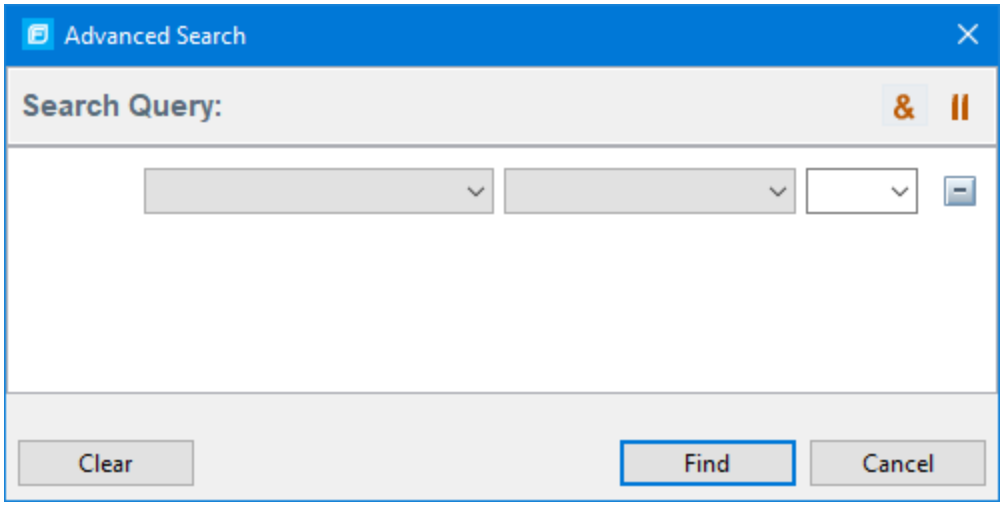
Search Target	Query
All privacy violations in file names that contain `jsp` with `getSSN()` as a source	`category:privacy violation source:getssn file:jsp`
All file names that contain `com/test/123`	`file:com/test/123`
All paths that contain traces with `mydbcode.sqlcleanse` as part of the name	`trace:mydbcode.sqlcleanse`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

Performing Advanced Searches

Use the advanced search feature to build complex search strings.

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 on the left, select a search modifier.
   b. From the middle list, select the comparison and type.
   c. From the list on the right, select a 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 box. 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 the **AND** button .
   - To add an OR query row, in the top right corner of the dialog box, click the **OR** button .
4. Add as many query rows as you need for the search query.
5. To delete a row, to the right of the row, click the **Delete** button . To remove all rows, click **Clear**.
6. To change a query row condition, double-click the current (underlined) query row operator **AND** or **OR**.

   In the following example, you can double-click **AND** to change the query operator to **OR**.

7. 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. **Find** is only enabled when the search query is error free.

About Issue Templates

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 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 tags 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 Fortify 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 in 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 85 and "Synchronizing Filter Sets and Folders" on page 86.

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. Select the **Filter Sets** tab.
3. Next to **Filter Sets**, click the **Add Filter Set** button  .
   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.

See Also

"Creating a Filter from the Static Analysis Results View" below

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 only created in the selected filter set.

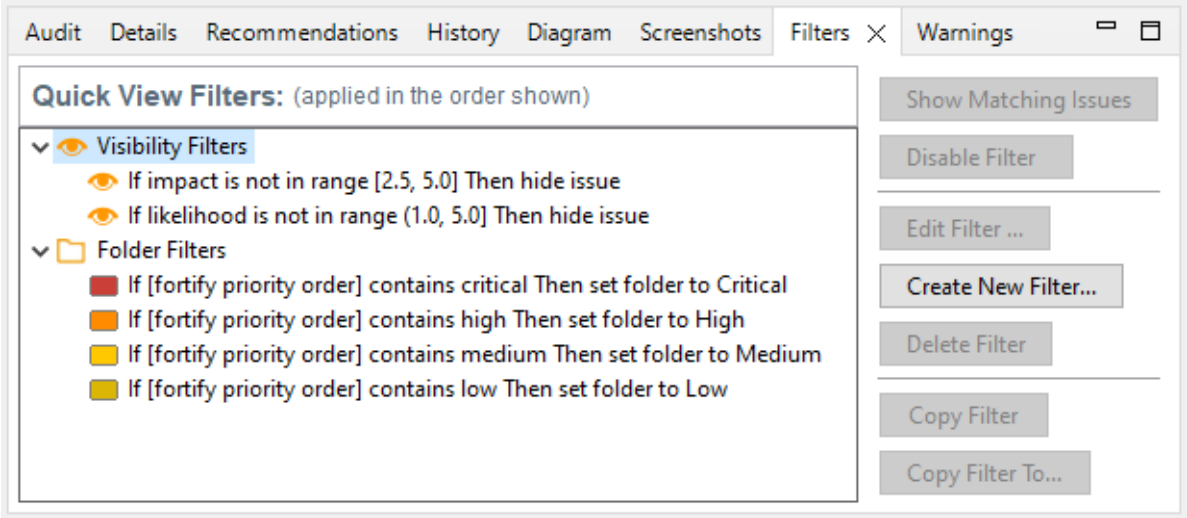
Creating a Filter from the Issue Auditing View

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.

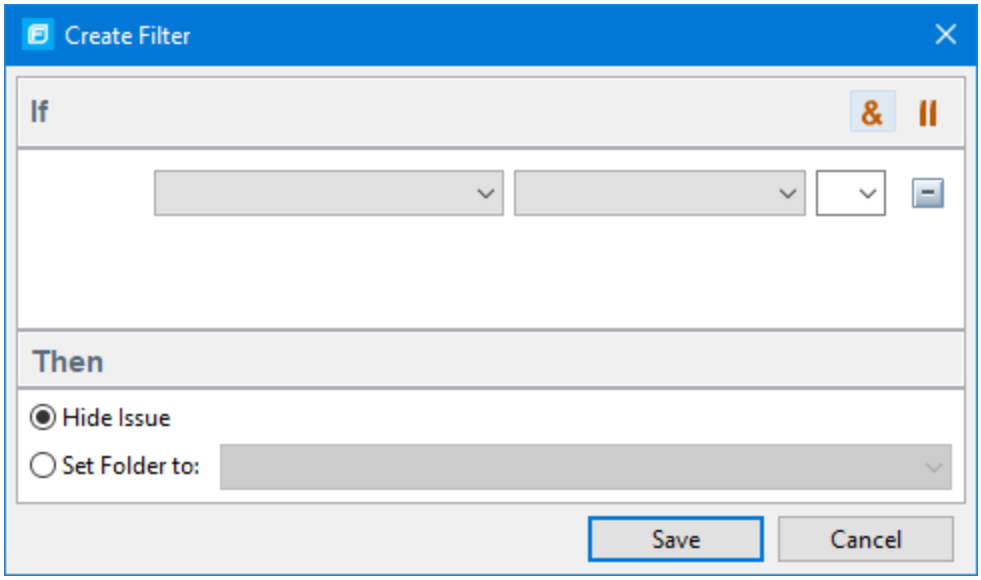
To create a new filter on the **Filters** tab:

1. From the **Filter Set** list, select a filter set.
2. Select 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.

   For a description of the available issue attributes, see "Search Modifiers" on page 72. The second list is then automatically populated with the available comparison methods.
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 only created in the selected filter set.

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. Select the **Filters** tab in the Issue Auditing view.
3. Right-click a filter, and then select **Copy Filter To**.

   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 in Fortify Software Security Center, do the following:

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

For information about logging into Fortify Software Security Center, see "Logging in to Fortify Software Security Center" on page 24.

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**.

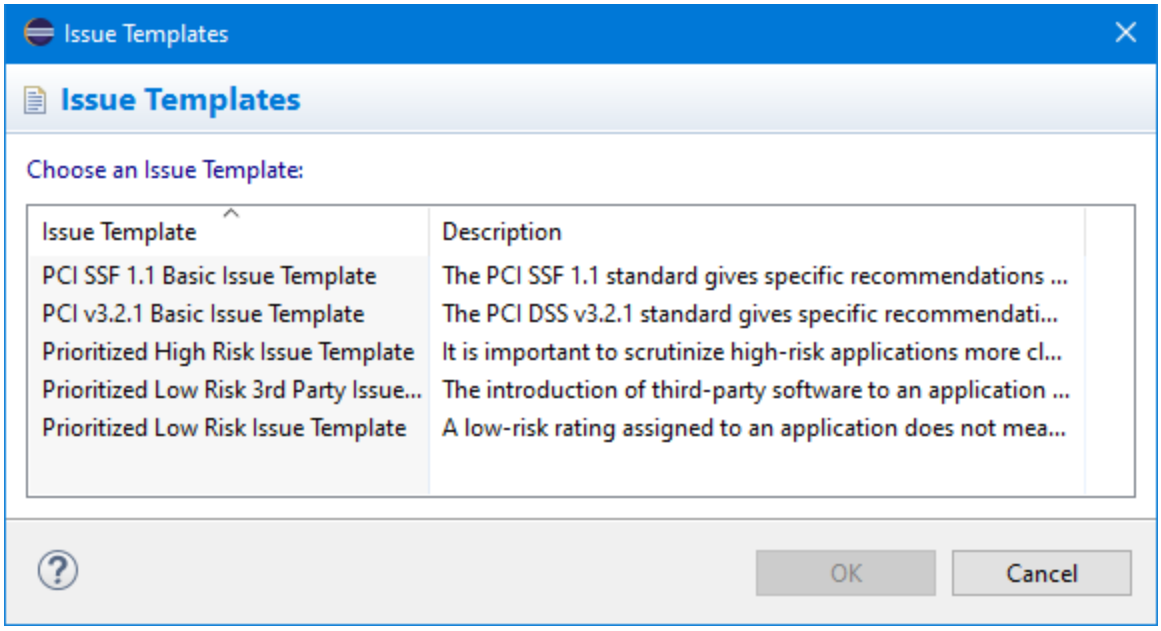
Synchronizing Filter Sets and Folders

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

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

   For information about logging into Fortify Software Security Center, see "Logging in to Fortify Software Security Center" on page 24.



If the current issue template does not exist in Fortify Software Security Center, do the following:

   a. In the **Issue Template** column, select an issue template name.
   b. Click **OK**.

6. The Fortify Eclipse Complete Plugin downloads the filter sets and folders from the selected issue template in 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

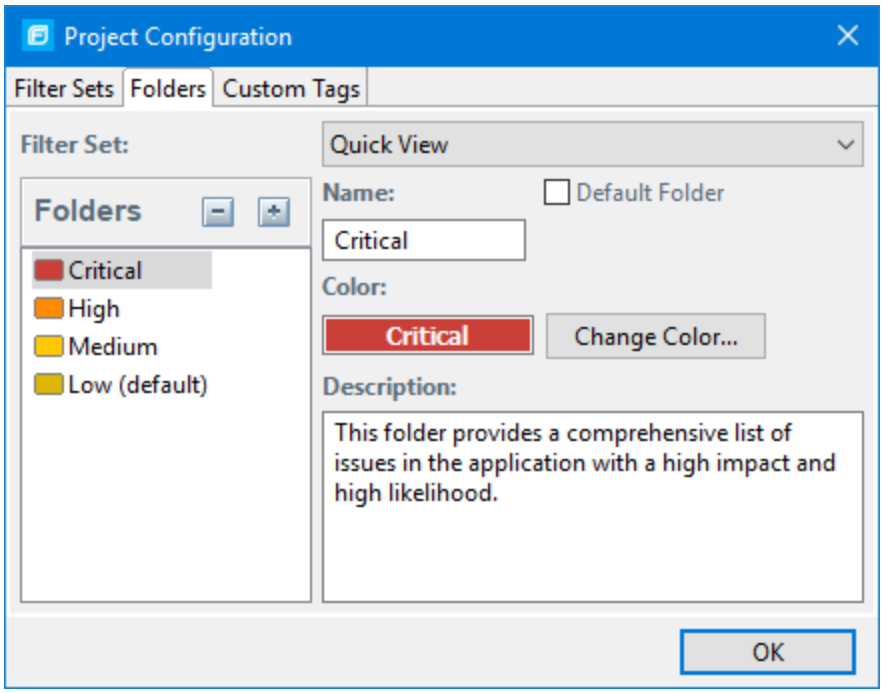
Folders are logical sets of issues that are defined by the filters in the active filter set. Even though a folder can appear in more than one filter set, the contents might differ depending on the filters in that filter set that target the folder. To accommodate filter sets that provide sorting mechanisms with little overlap, you can have filter sets with different folders. Folders are defined independent of the filter sets in which they might appear. 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. Select the **Folders** tab.
   The **Folders** pane 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 it with 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 the **Add Folder** button .

      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 82 and "Creating a Filter from the Issue Auditing View" on page 83.

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 is only included in the selected filter set using the instructions in "Creating a Folder" on page 87. 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. Select the **Folders** tab.
3. Click the **Filter Set** list to select the filter set where you want to add a folder.
   The **Folders** list displays the folders in the selected filter set.
4. Next to **Folders**, click the **Add Folder** button  .
   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.

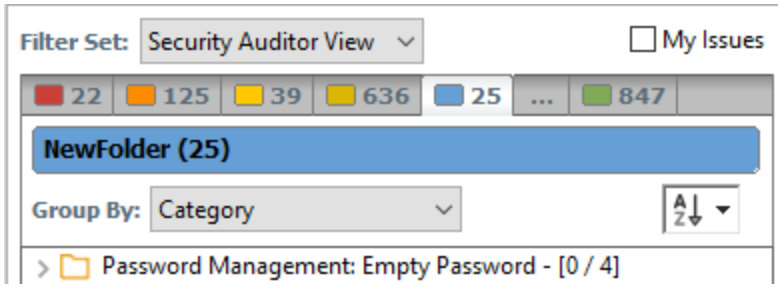
Renaming a Folder

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. Select 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 is displayed on the tab.



Removing a Folder

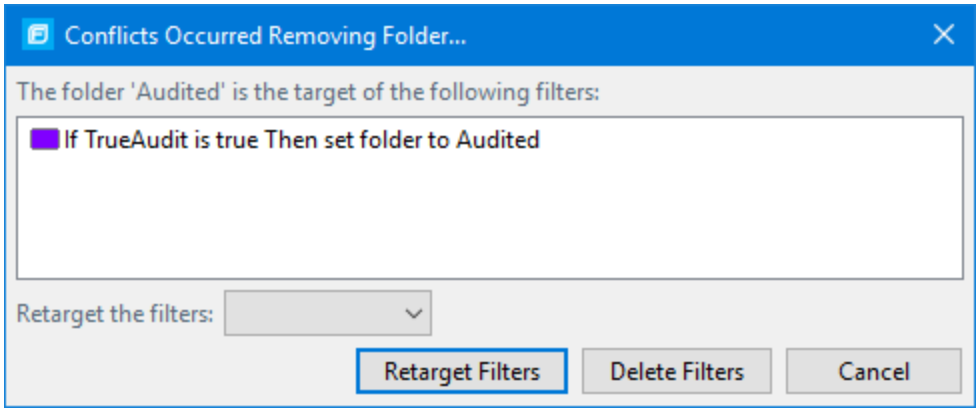
You can remove a folder from a filter set without removing it from other filter sets.

To remove a folder:

1. Select **Fortify > Project Configuration**.
2. Select 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 the **Delete Folder** button .

   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 Fortify Software Security Center, the security team examines project analysis 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 might 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.

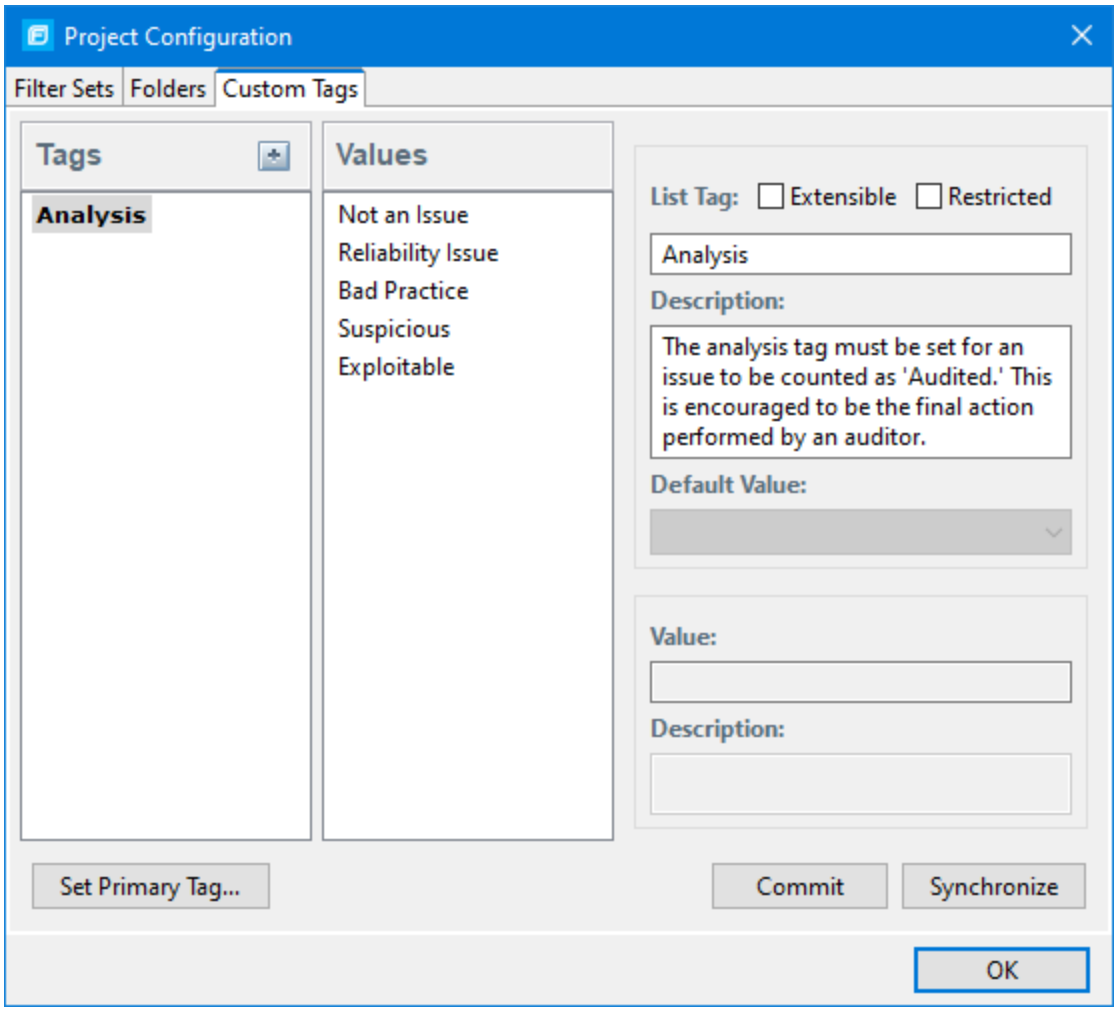
After you define a custom tag, it is displayed below the **Analysis** tag, which enables you to specify values as they relate to specific issues. Custom tags are also available in other areas of the interface, such as in the **Group By** list to group issues in a folder, in the search field as a search 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 the **Add Tag** button .

   Note: Any previously hidden tags 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 the **Add Value** button  .
   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 name is shown in bold in the **Tags** list. 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 **Audit** tab in the Issue Auditing view or as a search or filter option.

Note: If you hide a custom tag that was set for any issues, that tag and values are hidden from the issue. If you make the tag available again, the tag and values are restored.

You cannot hide the primary tag.

To hide a custom tag:

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

   The Project Configuration dialog box opens.
2. Select the **Custom Tags** tab.
3. Select the tag from the **Tags** list.

4. Next to **Tags**, click the **Hide Tag** button  .

   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 91).
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 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.

   For information about logging into Fortify Software Security Center, see "Logging in to Fortify Software Security Center" on page 24.

   The Custom Tag Upload dialog box opens.
5. Do one of the following:
   - If the issue template and the application version already exist in 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 in Fortify Software Security Center:
     - To upload the custom tags to the global pool only in 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 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.

   For information about logging into Fortify Software Security Center, see "Logging in to Fortify Software Security Center" on page 24.

   The Custom Tag Download dialog box opens.
6. If the application version and the issue template both exist in 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

After 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. Select 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**.

   Note: If any hidden custom tags exist in the template, you are prompted to indicate whether to include them in the exported issue template. Hidden tags are created anytime you add a custom tag and later delete it. Fortify Audit Workbench saves and hides deleted custom tags so you can easily restore them later. If you do not want hidden tags included in the exported issue template, click **Ignore Tags**.

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. Select 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.

Working with Issues

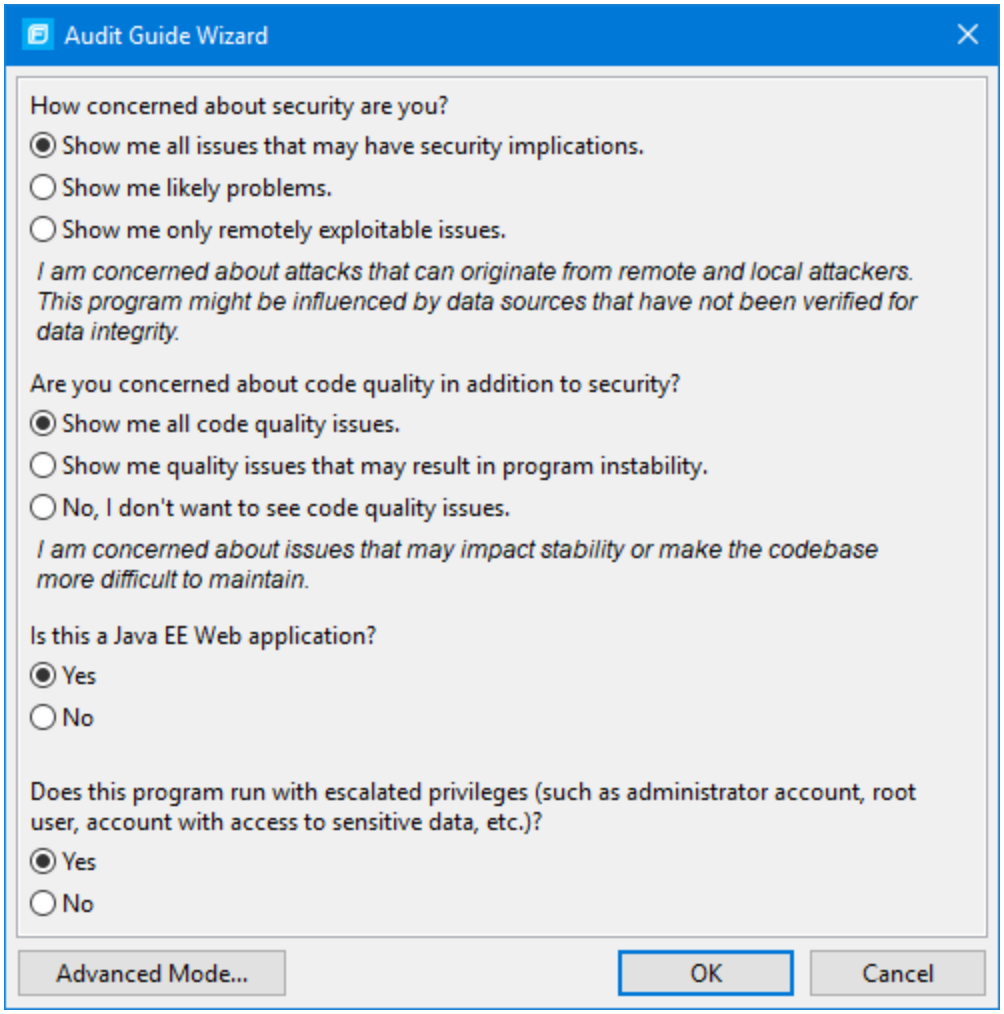
This section describes how to use the Fortify Eclipse Complete Plugin to review issues.

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.

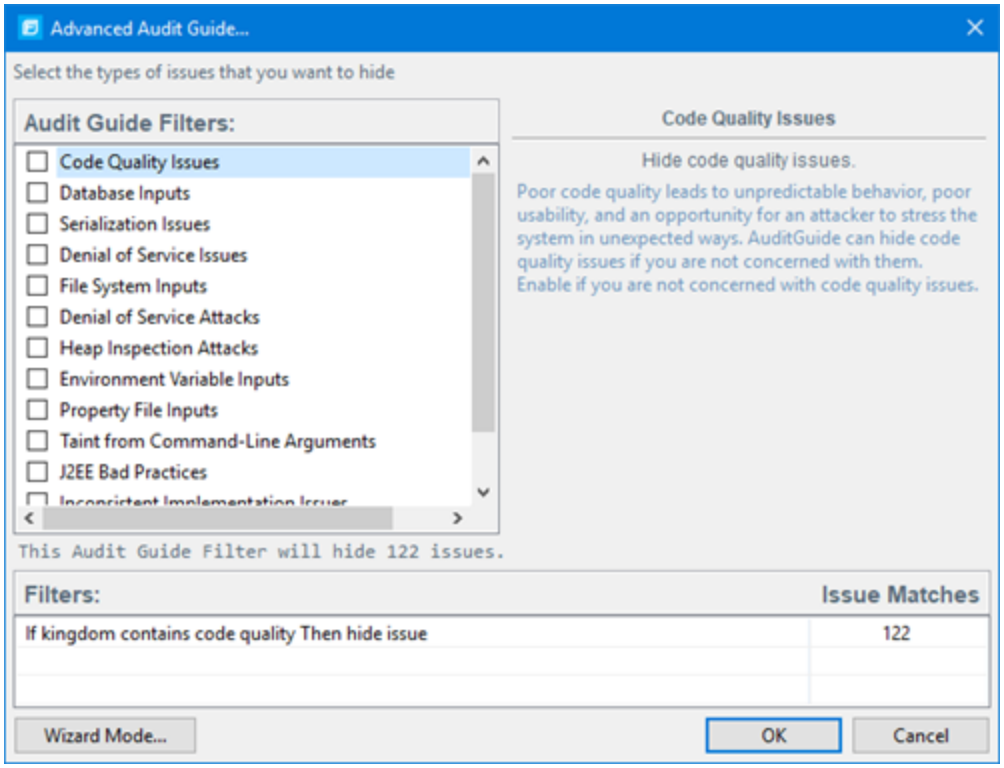
To use the Audit Guide:

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 **Static Analysis Results** view vary depending on the selected issue attribute. The attribute you select from the **Group By** list sorts issues in all visible folders into subfolders.

Use the issue attributes to group and view the issues in different ways. You can view issues with any of the available issue attributes, and you can create and edit customized groups. The following table describes the available issue attributes.

Issue Attribute	Description
Analysis	Groups issues by the audit analysis, such as Suspicious, Exploitable, and Not an Issue.

Issue Attribute	Description
Analysis Type	Groups issues by analyzer product, such as SCA, WEBINSPECT, and SECURITYSCOPE (Fortify WebInspect Agent).
Analyzer	Groups issues by analyzer group, such as Configuration, Control Flow, Data Flow, Pentest, Semantic, and Structural.
App Defender Protected	Groups issues by whether Application Defender can protect the vulnerability category.
Category	Groups issues by vulnerability category. This is the default grouping.
Category Analyzer	Groups issues by category and then by analyzer.
<custom_tagname>	Groups issues by custom tag.
File Name	Groups issues by file name.
Fortify Priority Order	Groups issues by Critical, High, Medium, and Low based on the issue priority.
Kingdom	Groups issues by the Seven Pernicious Kingdoms classification.
Manual	Groups issues by whether they were manually created by penetration test tools, and not automatically produced by a web crawler such as Fortify WebInspect.
<metadata_listname>	Groups issues by the alternative metadata external list names (for example, OWASP Top 10 *<year>*, CWE Top 25 *<year>*, PCI SSF *<version>*, STIG *<version>*, and others).
New Issue	Shows which issues are new since the last scan. For example, if you run a new scan, any issues that are new are displayed in the tree under the **Issue New** group and the others are displayed in the **Issue Updated** group. Issues not found in the latest scan are displayed in the **Issue Removed** group.
New Issue by Category	Groups issues that are new since the last scan and then by category. See also "New Issue" above.
Package	Groups issues by package or namespace. Nothing is shown for projects to which this option does not apply, such as C projects.
Priority by Category	Groups issues by Fortify Priority Order and then by category.

Issue Attribute	Description
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 file type. For dataflow issues, the file contains the sink function. **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 grouping option.

The following table describes additional grouping options that are available when you create a custom grouping option (see "Creating a Custom Grouping Option" on the next page).

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.
Source File	Groups dataflow issues by the source code file where the taint originated.
Status	Groups issues by the audit status (**Reviewed**, **Unreviewed**, or **Under Review**)
URL	Groups dynamic issues by the request web address.

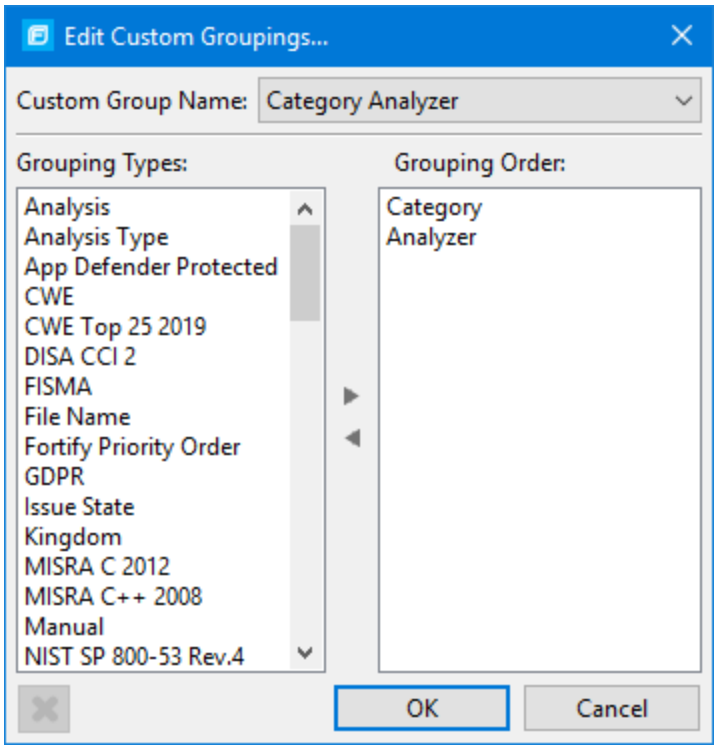
Creating a Custom Grouping Option

You can create a custom grouping option that groups issues in a hierarchical format in sequential order based on selected attributes.

To create a new grouping option:

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

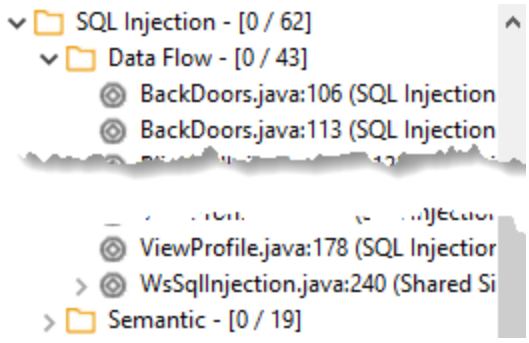
   The Edit Custom Groupings dialog box opens.



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 SQL Injection, with the issues grouped below by analyzer (such as Dataflow or Semantic).



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

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 pane, 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 pane, 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 pane, 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/en/java/index.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**.

Chapter 5: Auditing Analysis Results

Note: If your Fortify license restricts auditing, then you can view the analysis results, but you cannot audit issues or make any changes to the audit project.

The topics in this section provide information about how to audit analysis results opened in the Fortify Plugin for Eclipse.

This section contains the following topics:

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 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 previously-saved audit:

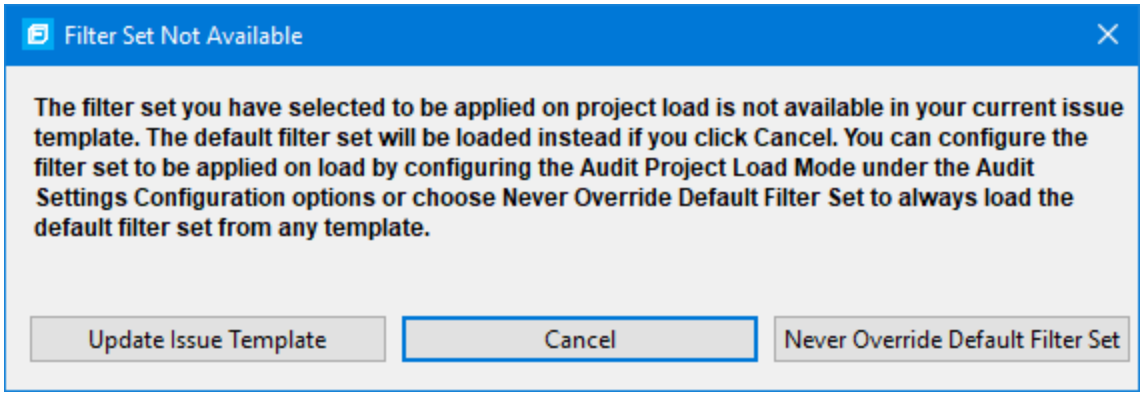
1. From Eclipse, select a project.
2. Select **Fortify > Load Saved Audit Project**.

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 OpenText™ Fortify on Demand.

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 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**.

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 Fortify Plugin for Eclipse 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 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 Fortify Plugin for Eclipse.
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 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 24.

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.

   For information about logging into Fortify Software Security Center, see "Logging in to Fortify Software Security Center" on page 24.
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 Analysis Results" on page 48.
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" below.

Refreshing Permissions from Fortify Software Security Center

The 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 Fortify Eclipse Complete Plugin.

To refresh your permissions from Fortify Software Security Center:

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

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 24.

When you work on a collaborative audit and you download the audit project from Fortify Software Security Center, the Fortify 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 94 and "Committing Filter Sets and Folders" on page 85 for more information.

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

For information about logging into Fortify Software Security Center, see "Logging in to Fortify Software Security Center" on page 24.

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 in Fortify Software Security Center to which Fortify Plugin 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 in Fortify Software Security Center) are uploaded.

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 Analysis Results" on page 48).

   Note: If multiple issues are selected, then this information is displayed on the **Audit** tab as **Issue: Multiple Issues Selected**.
2. Read the abstract on the **Audit** tab, which provides high-level information about the issue, such as the analyzer that found the issue.

   For example, **Command Injection (Input Validation and Representation, Data Flow)** indicates that this issue that the Dataflow Analyzer detected, is a Command Injection issue in the Input Validation and Representation kingdom.
3. Click the **Details** tab to see more details about the issue.
4. On the **Audit** tab, select an analysis value for the issue to represent your evaluation.
5. Specify values for any custom tags defined by your organization.

   To specify a date in a date-type custom tag, click the **Select Date** button to select a date from a calendar.

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

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

   Note: If you select a different value for the analysis tag than the **AA_Prediction** value set by Fortify Audit Assistant, and you select **Include** from the **AA_Training** list, then the next time the data is submitted to Fortify Audit Assistant, it updates the information used to predict whether an issue represents a true vulnerability. For more information about Fortify Audit Assistant, see the *OpenText™ 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 that you want to assign the same analysis value.
2. Press **Ctrl** + **Shift** + **A** (**Cmd** + **Shift** + **A** on macOS).

   The Fortify 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.

The Fortify Eclipse Complete Plugin provides keyboard shortcuts 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 pane, select **Audit Configuration**, and then select 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. The Fortify Eclipse Complete Plugin provides keyboard shortcuts 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.

See Also

"Configuring Custom Tags for Auditing" on page 91

Adding Screenshots to Issues

You can attach a screenshot or other image to an issue. Attached images are stored in the FPR file and are accessible from 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 pane, select the **Screenshots** tab.
3. Click **Add**.
4. In the New Screenshot dialog box, click **Browse** to find and select the file.
5. (Optional) In the **Description** box, type a description.
6. Click **Add**.

Viewing Images

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

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

1. In the Issue Auditing pane, select the **Screenshots** tab.
2. From the list of screenshots, click the image you want 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

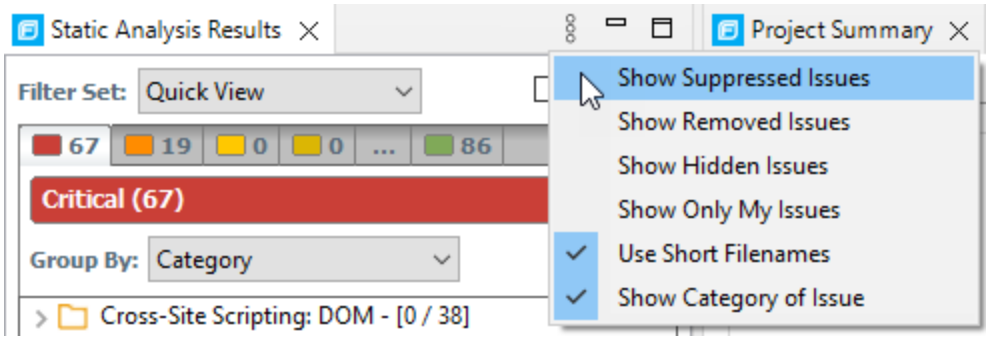
You can suppress issues that are either fixed or that you do not plan to fix. Suppression marks the issue and all future discoveries of this issue as suppressed. As such, it is a semi-permanent marking of a vulnerability.

To suppress 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 the **Suppress** button .
- 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.

To review results that have been suppressed, select **Show Suppressed Issues** from the **View Menu** button 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 the **Unsuppress** button .
- 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.

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 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 the **File Bug** button .
2. If this is the first time you have filed a bug, the Select Bug Tracker Integration dialog box opens. Select a bug tracker application, and then click **OK**.

   For information about configuring the plugin with bug tracker applications, see "Integrating with a Bug Tracker Application" on the next page.
3. 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 web address, product name, severity level, summary, and version.
4. If the connection to the bug tracker requires a proxy, select the **Use proxy** check box.

   With this option selected, the Fortify Plugin for Eclipse use the proxy settings specified for bug trackers. For more information, see "Configuring Proxy Settings for Bug Tracker Integration" on the next page.
5. Click **Submit**.

You must already be logged in 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** button  .
   The first time you submit a bug, the Select Bug Tracker 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 web address, product name, severity level, summary, and version.
3. Click **Submit**.

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

Integrating with a Bug Tracker Application

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

To select the plugin to use:

1. Open an audit project.
2. Select **Fortify > Select Bug Tracker**.
3. Select a bug tracker from the list, and then click **OK**.

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

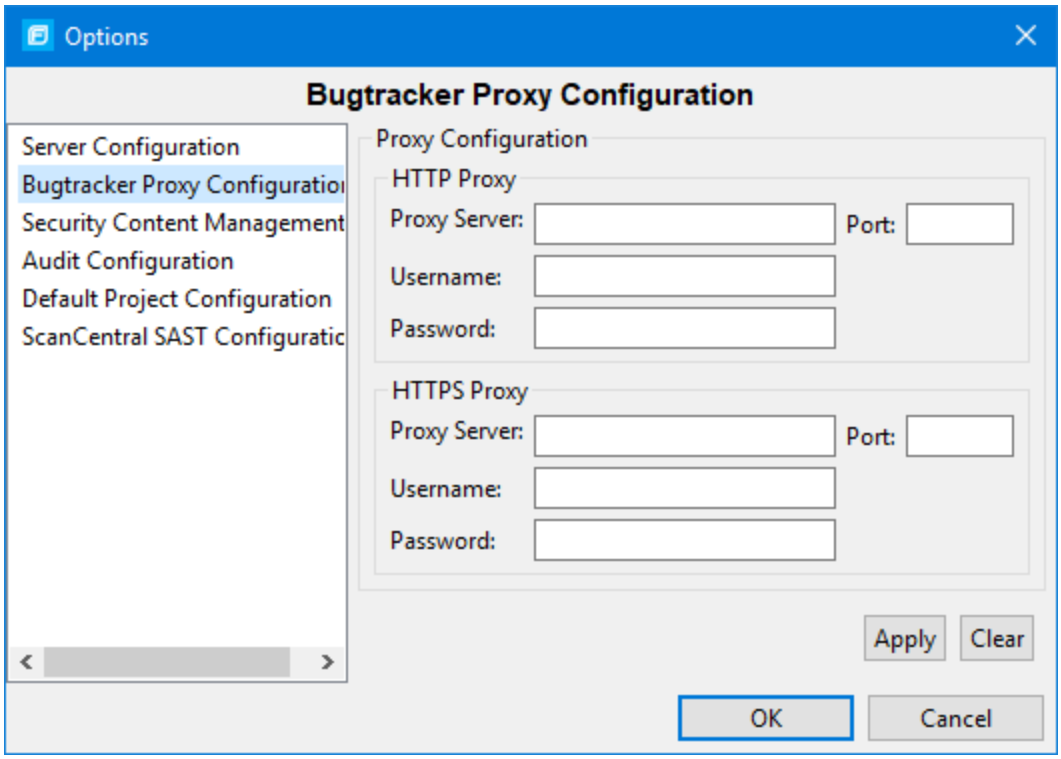
For bug tracker plugin components selected in the Fortify Applications and Tools installation, sample source code is available in `<tools_install_dir>/Samples/bugtrackers/BugTrackerPlugin<bug_tracker_app>`, where *<bug_tracker_app>* is the name of the bug tracker application. To write your own plugin, see the instructions in the `README` text file, which is in each bug tracker directory. A JavaDoc includes API information in `<tools_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 Plugin for Eclipse provides the proxy settings to the bug tracker plugin.

To configure proxy settings for bug tracker integration:

1. Select **Fortify > Options**.
2. In the left pane, 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.

Chapter 6: Generating Reports

The Fortify Plugin for Eclipse 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.

Generating Legacy Reports

After you select a report template and specify report settings, you generate the report to view the results. You can save the report results in PDF or XML format.

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.
6. Click **Save**.

   Fortify Plugin for Eclipse generates the report in the format you selected.

Legacy Report Templates

This section describes how to select and edit a legacy report template. 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 121). 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**—Provides 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**—Provides high-level information based on the category of issues that 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>***—Provides high-level summaries of uncovered vulnerabilities organized based on the top ten issues that the Open Web Security Project (OWASP) has identified.

The following sections describe how to view report templates and customize them to address your reporting needs.

Selecting Legacy Report Sections

You can choose sections to include in the report.

To select the sections that you want to include in a report:

1. Click a section title to view the contents of the section.
   The section details are displayed to the right of the dialog box.
2. To include a section in the report, select the section title check box in the list on the left side.
3. To remove a section from the report, clear the check box next to the section title.

For instructions on how to edit each section, see "Editing Legacy Report Subsections" below.

Opening Legacy Report Templates

To open a report template:

1. Select **Fortify > Generate Legacy Report**.
   The Generate Legacy Report dialog box opens.
2. From the **Report** list, select a report template to open.

The Generate Legacy Report dialog box displays the report template settings.

Editing Legacy Report Subsections

When you select a section title, you can edit the contents that are displayed 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:

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

2. Click **Edit Text**.
   The text box displays the text and variables to include in the report.
3. Edit the text and text variables.

As you edit text subsections, you can insert variables that are defined when you run the report. The following table describes these 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)
`$FILE_LISTING$`	List of scanned files, each in the 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
`$FORTIFY_SCA_VERSION$`	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)

Variable	Description
$RESULTS_CERTIFICATION_SUMMARY$	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
$SOURCE_BASE_PATH$	Source base path of codebase
$TOTAL_FINDINGS$	Number of issues, not including suppressed and removed issues
$VERSION_LABEL$	Label of the scanned project (available only if the Fortify Static Code Analyzer `-build-label` option was used in the scan)
$WARNINGS$	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 is displayed below the subsection title.
2. Click the issues list heading to expand the options.
3. Select the attributes used to group the results list.
   If you group by category, the recommendations, abstract, and explanation for the category are also included in the report. For the list of attributes to group by, see "Grouping Issues" on page 98.

4. (Optional) To refine the issues shown in this subsection with a search query, click **Advanced**.
   For information about the search syntax, see "Search Syntax" on page 71.
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 Chart 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 "Grouping Issues" on page 98.
3. (Optional) To refine the issues shown in this subsection with a search query, click **Advanced**.
   For information about the search syntax, see "Search Syntax" on page 71.
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**.

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 Legacy 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 folder that contains 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.png` and `footer.png` in this directory.

Adding Legacy Report Sections

You can add report sections by editing the XML files. In the XLM structure, the `ReportSection` element defines a new section. It includes a `Title` element for the section name, and it must include at least one `Subsection` element 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="true" 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 for critical and high priority issues.
      Vulnerability examples are provided by category.
    </Description>
    <IssueListing limit="1" listing="true">
      <Refinement>[fortify priority order]:critical OR
        [fortify priority order]:high</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 second subsection is a

results list named `Vulnerability Examples by Category`. A section can contain multiple subsections.

Adding Report Subsections

In the report sections, you can add subsections or edit subsection content. Subsections can generate text, results lists, or charts.

Adding Text Subsections

In a text subsection, you can include the `Title` element, the `Description` element, and the `Text` element. In the `Text` element, 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 Legacy Report Subsections" on page 117. 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 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` element, the `Description` element, and the `IssueListing` element. In the `IssueListing` element, you can define the default content for the limit and set `listing` to `true`. You can include the `Refinement` element 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` element attribute `chartType` is set to `list`. You can also define the `Axis` element. The following XML is the `Vulnerability 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>[fortify priority order]:critical OR
      [fortify priority order]:high</Refinement>
    <Chart chartType="list">
      <Axis>Category</Axis>
    </Chart>
  </IssueListing>
</SubSection>
```

In this example, the results list subsection is titled `Vulnerability Examples by Category`. The 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` element value) where there are issues that match the statement `[fortify priority order]:critical OR [fortify priority order]:high` (the value of the `Refinement` element).

Adding Charts Subsections

In a chart subsection, you can include the `Title` element, the `Description` element, and the `IssueListing` element. In the `IssueListing` element, you can define the default content for the limit and set `listing` to `false`. You can include the `Refinement` element either with or without a default statement, although you can edit the content before generating a report. To generate a pie chart, the `Chart` element's 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` element.

The following code shows an example of a chart 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` element is empty) and groups the issues on the value of `New Issues` (the value of the `Axis` element). This chart is displayed as a pie chart (`chartType="pie"`).

Chapter 7: Troubleshooting

The following topics provide information on how to troubleshoot problems you might encounter working with the Fortify Plugin for Eclipse.

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 Local Analysis Options" on page 28).

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 Fortify Plugin for Eclipse displays following warning message:

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

Click **Limit** to limit the number of issues to the maximum or click **Save All** to save all the removed issues. The `com.fortify.RemovedIssuePersistanceLimit` property controls the maximum

number of removed issues <*removed_issues_limit*>. See the *OpenText™ Fortify Static Code Analyzer Applications and Tools Guide* for more information.

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

1. Select **Fortify > Options**.
2. In the left pane, select **Audit Configuration**.
3. Select 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 Debug Option

If you encounter errors, you can enable the debug 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
Fortify Plugin for Eclipse	<*eclipse_install_dir*>/plugins/com.fortify.dev.ide.eclipse_<*version*>/Core/config

2. You can either enable debug mode for all Fortify Applications and Tools or for specific applications. 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 Applications and 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 Fortify Plugin for Eclipse runs in debug mode.

Locating Log Files

For help diagnosing a problem, provide log files to Customer Support. In addition to the Fortify log files described in this topic, also consider providing the Eclipse error log file stored in the workspace's `.metadata` directory.

On Windows systems, the default Fortify log files are the following directories:

- `C:\Users\<username>\AppData\Local\Fortify\sca<version>\log`
  The log files in this directory are only available if you analyze the code locally with Fortify Static Code Analyzer.
- `C:\Users\<username>\AppData\Local\Fortify\Eclipse.Plugin-<version>\log`
- `C:\Users\<username>\AppData\Local\Fortify\scancentral-<version>\log`
  The log files in this directory are only available if you analyze the code with Fortify ScanCentral SAST.

On Linux and macOS systems, the default Fortify log files are the following directories:

- `<userhome>/.fortify/sca<version>/log`
  The log files in this directory are only available if you analyze the code locally with Fortify Static Code Analyzer.
- `<userhome>/.fortify/Eclipse.Plugin-<version>/log`
- `<userhome>/.fortify/scancentral-<version>/log`
  The log files in this directory are only available if you analyze the code with Fortify ScanCentral SAST.

Send Documentation Feedback

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

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

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

Feedback on User Guide (Fortify Plugin for Eclipse 24.4.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!