

OpenText™ Fortify Audit Workbench

Software Version: 24.2.0

User Guide

Document Release Date: May 2024

Software Release Date: May 2024

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 2004 - 2024 Open Text.

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

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

This document was produced for OpenText™ Fortify Audit Workbench CE 24.2 on May 15, 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	9
Contacting Customer Support	9
For More Information	9
About the Documentation Set	9
Fortify Product Feature Videos	9
 Change Log	 10
 Chapter 1: Introduction	 12
About Fortify Audit Workbench	12
Audit Projects and Issue Templates	12
Hybrid 2.0 Technology	13
Integration with Fortify Static Code Analyzer	13
Integration with Fortify Software Security Center	13
Related Documents	14
All Products	14
Fortify Software Security Center	15
Fortify Static Code Analyzer	15
Fortify Static Code Analyzer Applications and Tools	16
 Chapter 2: Getting Started	 18
Installing Fortify Audit Workbench	18
About Upgrades	18
Upgrading Manually	19
Configuring Automatic Upgrades	19
Sample Projects	20
Renewing Expired Licenses	20
About Starting Fortify Audit Workbench	21
Starting Fortify Audit Workbench on Windows Systems	21
Starting Fortify Audit Workbench on Non-Windows Systems	21
Changing the Appearance	21

Working with Fortify Software Security Center	22
Configuring a Connection to Fortify Software Security Center	22
Logging in to Fortify Software Security Center	22
Fortify Software Security Content	24
Configuring Security Content Updates	24
Updating Security Content	26
Importing Custom Security Content	28
Chapter 3: Scanning Source Code	29
Scanning Java Projects	29
About Quick Scan Mode	31
Scanning Large and Complex Projects	31
Scanning Visual Studio Solutions	35
Rescanning Projects	37
Chapter 4: Viewing Analysis Results	39
About Viewing Analysis Results	39
Issues View	40
Filter Sets	41
Specifying the Default Filter Set	41
Folders (Tabs)	42
Group By List	43
Specifying the Default Issue Grouping	43
Sorting Issues	44
Search Box	44
Project Summary View	45
Summary Tab	45
Certification Tab	45
Build Information Tab	45
Analysis Information Tab	45
Viewing Summary Graph Information	46
Source Code Tab	49
About Displayed Source Code	50
Analysis Trace View	50
Issue Auditing View	52
Audit Tab	53
Details Tab	54

WebInspect Agent Details Tab	55
Recommendations Tab	55
History Tab	55
Diagram Tab	55
Filters Tab	56
Warnings Tab	57
Functions View	59
Customizing the Issues View	59
Searching for Issues	61
Search Syntax	62
Search Modifiers	63
Search Query Examples	70
Performing Advanced Searches	70
Working with Issues	72
Filtering Issues with Audit Guide	72
Grouping Issues	73
Creating a Custom Grouping Option	76
Using Smart View	77
Selectively Displaying Issues Assigned to You	79
About Suppressed, Removed, and Hidden Issues	80
Creating Attribute Summary Tables for Multiple Issues	80
About Issue Templates	82
Configuring Custom Filter Sets and Filters	83
Creating a New Filter Set	83
Creating a Filter from the Issues View	84
Creating a Filter from the Issue Auditing View	85
Copying a Filter from One Filter Set to Another	86
Setting the Default Filter Set	86
Managing Folders	87
Creating a Folder	87
Adding a Folder to a Filter Set	89
Renaming a Folder	89
Removing a Folder	90
Configuring Custom Tags for Auditing	91
Adding a Custom Tag	91
Hiding a Custom Tag	93
Committing Custom Tags to Fortify Software Security Center	94

Synchronizing Custom Tags with Fortify Software Security Center	95
Issue Template Sharing	95
Exporting an Issue Template	95
Importing an Issue Template	96
Synchronizing Filter Sets and Folders	96
Committing Filter Sets and Folders	97
Advanced Configuration	98
Integrating with a Bug Tracker Application	98
Configuring Proxy Settings for Bug Tracker Integration	98
Public APIs	99
Penetration Test Schema	99
Chapter 5: Auditing Analysis Results	100
Working with Audit Projects	100
Opening an Audit Project	100
Opening Audit Projects Without the Default Filter Set	101
Performing a Collaborative Audit	101
Refreshing Permissions from Fortify Software Security Center	102
Merging Audit Data	102
Merging Audit Data Using the Command-Line Utility	103
Additional Metadata	103
Uploading Audit Results to Fortify Software Security Center	103
Evaluating Issues	104
Performing Quick Audits	105
Performing Quick Audits for Custom Tags	106
Adding Screenshots to Issues	106
Viewing Images	107
Creating Issues for Undetected Vulnerabilities	107
Suppressing Issues	107
Submitting an Issue as a Bug	108
Correlation Justification	109
Using Correlation Justification	109
Penetration Test Results	112
Viewing Penetration Test Results	113
Chapter 6: Generating Analysis Reports	114

Issue Reports	114
Generating Issue Reports	116
Legacy Reports and Templates	118
Generating Legacy Reports	119
Legacy Report Templates	119
Selecting Legacy Report Sections	119
Opening Legacy Report Templates	120
Editing Legacy Report Subsections	121
Editing Text Subsections	122
Editing Results List Subsections	123
Editing Chart Subsections	124
Saving Legacy Report Templates	124
Saving Changes to Legacy Report Templates	124
Report Template XML Files	125
Adding Legacy Report Sections	125
Adding Report Subsections	126
Adding Text Subsections	126
Adding Results List Subsections	127
Adding Charts Subsections	127
Chapter 7: Using the Functions View	129
Opening the Functions View	130
Sorting and Viewing Functions	131
Locating Functions in Source Code	132
Synchronizing the Functions View with the Analysis Trace View	132
Locating Classes in Source Code	132
Determining Which Rules Matched a Function	133
Writing Rules for Functions	133
Creating Custom Cleanse Rules	134
Chapter 8: Troubleshooting	135
Creating Archive Logs for Customer Support	135
Using the Debug Option	135
Locating Log Files	136
Addressing the org.eclipse.swt.SWTError Error	136

Out of Memory Errors	137
Allocating Additional Memory for Fortify Audit Workbench	137
Allocating Additional Memory for Fortify Static Code Analyzer	137
Specifying Memory for External Processes	138
Saving a Project that Exceeds the Maximum Removed Issues Limit	138
Resetting the Default Views	139
Appendix A: Static Analysis Results Prioritization	140
About Results Prioritization	140
Quantifying Risk	141
Estimating Impact and Likelihood with Input from Rules and Analysis	142
Appendix B: Legacy Report Components	145
Fortify Security Report	145
Fortify Developer Workbook Report	148
OWASP Top Ten Reports	149
Fortify Scan Summary Report	150
Send Documentation Feedback	152

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
24.2.0	<p>Updated:</p> <ul style="list-style-type: none">• Added a timeout setting for downloading analysis results from Fortify Software Security Center (see "Configuring a Connection to Fortify Software Security Center" on page 22)• The unused metric executable lines of code is no longer displayed in the Project Summary view (see "Project Summary View" on page 45)• Added search modifier engine priority (see "Search Modifiers" on page 63)• Added New Issues by Category grouping attribute (see "Grouping Issues" on page 73)
23.2.0	<p>Added:</p> <ul style="list-style-type: none">• "Integration with Fortify Static Code Analyzer" on page 13 <p>Updated:</p> <ul style="list-style-type: none">• Added descriptions for the OWASP MASVS 2.0 and OWASP API Top 10 reports (see "Issue Reports" on page 114)
23.1.0	<p>Updated:</p> <ul style="list-style-type: none">• Changes were made throughout this guide for the introduction of a separate OpenText™ Fortify Static Code Analyzer Applications and Tools installer• Changed location for sample bug tracker plugins (see "Integrating with a Bug Tracker Application" on page 98)
22.2.0	<p>Updated:</p> <ul style="list-style-type: none">• The ability to restrict auditing capabilities was added to the Fortify license (see "About Fortify Audit Workbench" on page 12).

Software Release / Document Version	Change
	<ul style="list-style-type: none">• The location of the sample bug tracker plugins has changed (see "Integrating with a Bug Tracker Application" on page 98).• Sample projects are no longer included with the Fortify Static Code Analyzer and Applications installer. The samples are provided as a separate package (see "Sample Projects" on page 20).

Chapter 1: Introduction

This section contains the following topics:

- [About Fortify Audit Workbench](#) 12
- [Integration with Fortify Static Code Analyzer](#) 13
- [Integration with Fortify Software Security Center](#) 13
- [Related Documents](#) 14

About Fortify Audit Workbench

Fortify Audit Workbench complements OpenText™ Fortify Static Code Analyzer with a graphical user interface you can use to scan software projects and to organize, investigate, and prioritize the analysis results so that your team can fix security issues quickly and effectively.

From Fortify Audit Workbench, you can view and audit Fortify Project Results (FPR files) from OpenText™ Fortify Software Security Center, and Fortify Secure Code Plugins. Fortify Audit Workbench issue templates help you sort the results of large scans in a way that works for your business and workflows.

Note: If your Fortify license restricts auditing, then you can scan your code, view audit projects (FPR files), and generate reports from Fortify Audit Workbench, but you cannot audit issues or make any changes to the audit project. You also cannot upload audit projects to Fortify Software Security Center. You can open and review collaborative audits in Fortify Software Security Center, but you cannot make any changes.

Audit Projects and Issue Templates

After you initiate a source code scan from Fortify Audit Workbench, 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 Fortify Audit Workbench (and Fortify Software Security Center) configures and prioritizes the vulnerabilities (issues) uncovered in source code. Fortify Audit Workbench 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 Fortify Audit Workbench.

Hybrid 2.0 Technology

The Fortify Audit Workbench Hybrid 2.0 technology connects penetration test results directly to source code analysis results to reveal hidden vulnerability relationships and expose their root causes within the source code. This enables your security and development teams to more accurately identify and prioritize vulnerabilities, and more productively investigate and remediate security issues in the source code.

Integration with Fortify Static Code Analyzer

You can analyze your code with Fortify Static Code Analyzer from Fortify Audit Workbench. 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 Fortify Audit Workbench) 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

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 Fortify Audit Workbench 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
- Check for and install available upgrades of Fortify Static Code Analyzer and associated applications (including Fortify Audit Workbench)
- Download issue templates
- Upload new and modified issue templates

See Also

["Working with Fortify Software Security Center" on page 22](#)

["Configuring a Connection to Fortify Software Security Center" on page 22](#)

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
<i>About Fortify Software Documentation</i> 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.
<i>Fortify Software System Requirements</i> Fortify_Sys_Reqs_<version>.pdf	This document provides the details about the environments and products supported for this version of Fortify Software.
<i>Fortify Software Release Notes</i> 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.
<i>What's New in Fortify Software <version></i> Fortify_Whats_New_<version>.pdf	This document describes the new features in Fortify Software products.

Fortify Software Security Center

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

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

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
<i>OpenText™ Fortify Static Code Analyzer User Guide</i> SCA_Guide_<version>.pdf	This document describes how to install and use Fortify Static Code Analyzer to scan code on many of the major programming platforms. It is intended for people responsible for security audits and secure coding.
<i>OpenText™ Fortify Static Code Analyzer Applications and Tools Guide</i> 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.

Document / File Name	Description
<i>OpenText™ Fortify Static Code Analyzer Custom Rules Guide</i> SCA_Cust_Rules_Guide_<version>.zip	This document provides the information that you need to create custom rules for Fortify Static Code Analyzer. This guide includes examples that apply rule-writing concepts to real-world security issues. Note: This document is included only with the product download.
<i>OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide</i> 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. Unless otherwise noted, 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
<i>OpenText™ Fortify Audit Workbench User Guide</i> 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.
<i>OpenText™ Fortify Plugin for Eclipse User Guide</i> Eclipse_Plugin_Guide_<version>.pdf	This document provides information about how to install and use the Fortify Complete Plugin for Eclipse.
<i>OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studio User Guide</i> IntelliJ_AnalysisPlugin_Guide_<version>.pdf	This document describes how to install and use Fortify Analysis Plugin for IntelliJ IDEA and Android Studio.

Document / File Name	Description
<i>OpenText™ Fortify Extension for Visual Studio User Guide</i> 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 provide an overview of Fortify Audit Workbench, instructions on how to start the tool, and instructions on how to upgrade the Static Code Analyzer and Applications (Fortify Static Code Analyzer, Fortify Audit Workbench, and any plugins or extensions you have installed) as new versions of the products become available.

This section contains the following topics:

- [Installing Fortify Audit Workbench](#) 18
- [About Upgrades](#) 18
- [Sample Projects](#) 20
- [Renewing Expired Licenses](#) 20
- [About Starting Fortify Audit Workbench](#) 21
- [Changing the Appearance](#) 21
- [Working with Fortify Software Security Center](#) 22
- [Fortify Software Security Content](#) 24

Installing Fortify Audit Workbench

You install Fortify Audit Workbench by selecting it as a component when you install Fortify Static Code Analyzer Applications and Tools. For detailed installation instructions, see the *OpenText™ Fortify Static Code Analyzer Applications and Tools Guide*.

Fortify Audit Workbench uses the license provided during the Fortify Applications and Tools installation.

About Upgrades

You can check on the availability of new versions of Fortify Static Code Analyzer or Fortify Applications and Tools directly from Fortify Audit Workbench. If a version newer than the one you have installed is available from your Fortify Software Security Center server, you can download it and upgrade your instance.

You can also configure Fortify Audit Workbench to check for, download, and install new versions automatically at startup. Whether you upgrade Fortify Static Code Analyzer or Fortify Applications and Tools manually or automatically, Fortify Audit Workbench preserves your data.

To enable upgrades from Fortify Audit Workbench, a Fortify Software Security Center administrator must first set up the automatic upgrade capability on the Fortify Software Security Center server. For instructions on how to do this, see the *OpenText™ Fortify Software Security Center User Guide*.

Upgrading Manually

You can check for newer versions of Fortify Static Code Analyzer or Fortify Applications and Tools manually, from either the Fortify Audit Workbench **Help** menu or the Options dialog box.

To check for, and (potentially) install, a newer version of Fortify Static Code Analyzer or Fortify Applications and Tools :

1. Select **Options > Options**.

The Options dialog box opens to the **Server Configuration** settings.

2. Under **Audit Workbench Upgrade Configuration**, do the following:

- a. In the **Server URL** box, type the web address for the installers folder on your Fortify Software Security Center server (for example,
`https://my.domain.com:8080/ssc/update-site/installers`).

Note: If your Fortify Software Security Center administrator set up the automatic upgrade capability using an XML file other than `update.xml`, then you must include the XML file in the **Server URL** box (for example,
`https://my.domain.com:8080/ssc/update-site/installers/<update_config_file>.xml`).

- b. Click **Check Now**.

Note: You can also select **Help > Check for Upgrades** after you set up a Fortify Software Security Center installer web address described in the previous step.

The Fortify Audit Workbench polls the upgrade server for information about the Fortify Static Code Analyzer or Fortify Applications and Tools versions available for the platform on which it is running. If a newer version is available, Fortify Audit Workbench prompts you to indicate whether you want to proceed to download and install it.

Important! If you have the OpenText™ Fortify Plugin for Eclipse installed, after you upgrade Fortify Static Code Analyzer Applications and Tools from Fortify Audit Workbench, you must uninstall, and then reinstall the Fortify Plugin for Eclipse.

Configuring Automatic Upgrades

To configure upgrade checks at Fortify Audit Workbench startup:

1. From Fortify Audit Workbench, select **Options > Options**.

The Options dialog box opens to the **Server Configuration** settings.

2. Under **Audit Workbench Upgrade Configuration**, do the following:

- a. In the **Server URL** box, type the web address for the installers folder on your Fortify Software Security Center server (for example,
`https://my.domain.com:8080/ssc/update-site/installers`).

Note: If your Fortify Software Security Center administrator set up the automatic upgrade capability using an XML file other than `update.xml`, then you must include the XML file in the **Server URL** box (for example, `https://my.domain.com:8080/ssc/update-site/installers/<update_config_file>.xml`).

- b. Select the **Check for upgrades at startup** check box.
3. Click **OK**.

Each time you start Fortify Audit Workbench, it checks the server to determine if a newer Fortify Static Code Analyzer or Fortify Applications and Tools version is available and then, if a newer version is available, downloads and installs it.

Important! If you have a Fortify Plugin for Eclipse installed, after you upgrade your Fortify Applications and Tools from Fortify Audit Workbench, you must uninstall, and then reinstall the Fortify Plugin for Eclipse.

Sample Projects

The Fortify Applications and Tools installation includes a sample Fortify Project Results (FPR) file in `<tools_install_dir>/Samples/fprs`.

Fortify also provides several code samples in a separate download in the `Fortify_SCA_Samples_<version>.zip` archive. You can use these sample projects when learning to use Fortify Static Code Analyzer and Fortify Audit Workbench. The ZIP contains two directories: `basic` and `advanced`. Each code sample includes a `README.txt` file that provides instructions on how to scan the code in Fortify Static Code Analyzer and view the output in Fortify Audit Workbench.

The `basic` directory includes an assortment of simple language-specific code samples. The `advanced` directory contains more advanced samples.

Renewing Expired Licenses

The license for Fortify Audit Workbench expires annually. For information about how to obtain a Fortify license file, see the *Fortify Software System Requirements* document.

To update an expired license:

1. Put the updated Fortify license file in the `<tools_install_dir>` folder.
2. Start Fortify Audit Workbench and verify that it opens successfully.

About Starting Fortify Audit Workbench

You can start Fortify Audit Workbench from the start menu on a Windows system. You can start it from the command line on any supported operating system.

Starting Fortify Audit Workbench on Windows Systems

To start Fortify Audit Workbench on a Windows system, do one of the following:

- Select **Start > All Programs > Fortify Applications and Tools <version> > Audit Workbench**.
- Start Fortify Audit Workbench from the command line:
 - a. Open a Command window.
 - b. At the prompt, type `auditworkbench`.

Starting Fortify Audit Workbench on Non-Windows Systems

To start Fortify Audit Workbench on a Linux system:

1. Open a command prompt window, and then navigate to the `<tools_install_dir>/bin` directory.
2. At the prompt, type `auditworkbench`.

To start Fortify Audit Workbench on macOS:

- In the `<tools_install_dir>` directory, click `AuditWorkbench.app`.

Changing the Appearance

Fortify Audit Workbench comes with a dark or light (default) theme.

To change the appearance:

1. Select **Options > Appearance** and select a theme.

Note: To reset the appearance to the default theme, select **Reset Interface**.

2. Restart Fortify Audit Workbench when prompted.

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 Fortify Static Code Analyzer Applications and Tools keystore. The keystore is in the `<tools_install_dir>/jre/lib/security/cacerts` file.

To configure a connection to Fortify Software Security Center:

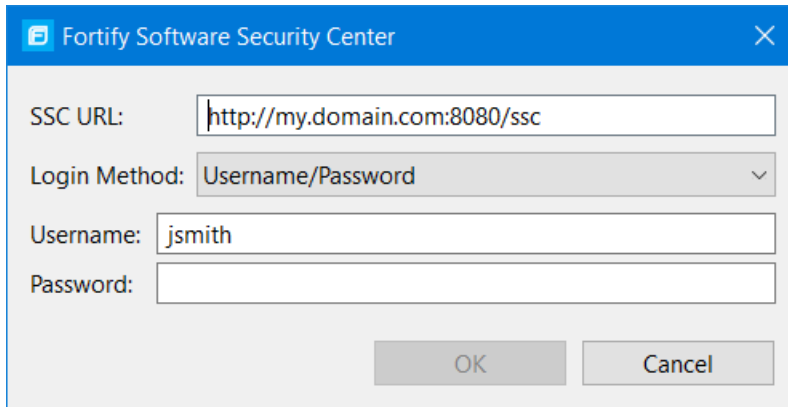
1. Select **Options > Options**.
2. In the left pane, select **Server Configuration**.
3. Under **Software Security Center Configuration**, specify the **Server URL** for your Fortify Software Security Center server.
4. If required, specify the proxy server, port number, and optionally credentials for 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 decoded value of a Fortify Software Security Center authentication token of type ToolsConnectToken. Note: For instructions about how to create an authentication token from Fortify Software Security Center, see the <i>OpenText™ Fortify Software Security Center User Guide</i> .
X.509 SSO	<ol style="list-style-type: none">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.

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)

Fortify 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.

Typically, you obtain the current Fortify Software Security Content when you install Fortify Static Code Analyzer.

Configuring Security Content Updates

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 26](#).

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

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

Server Configuration

Security Content Update

Update from Software Security Center
 Update from Fortify Update Server

Server URL:

Proxy Server: Port:

Username:

Password:

Update security content automatically
Update frequency (days)

Software Security Center

Server URL:

Proxy Server: Port:

Username:

Password:

Download Timeout (MS):

Audit Workbench Upgrade Configuration

Server URL:

Check for upgrades at startup

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 28](#)

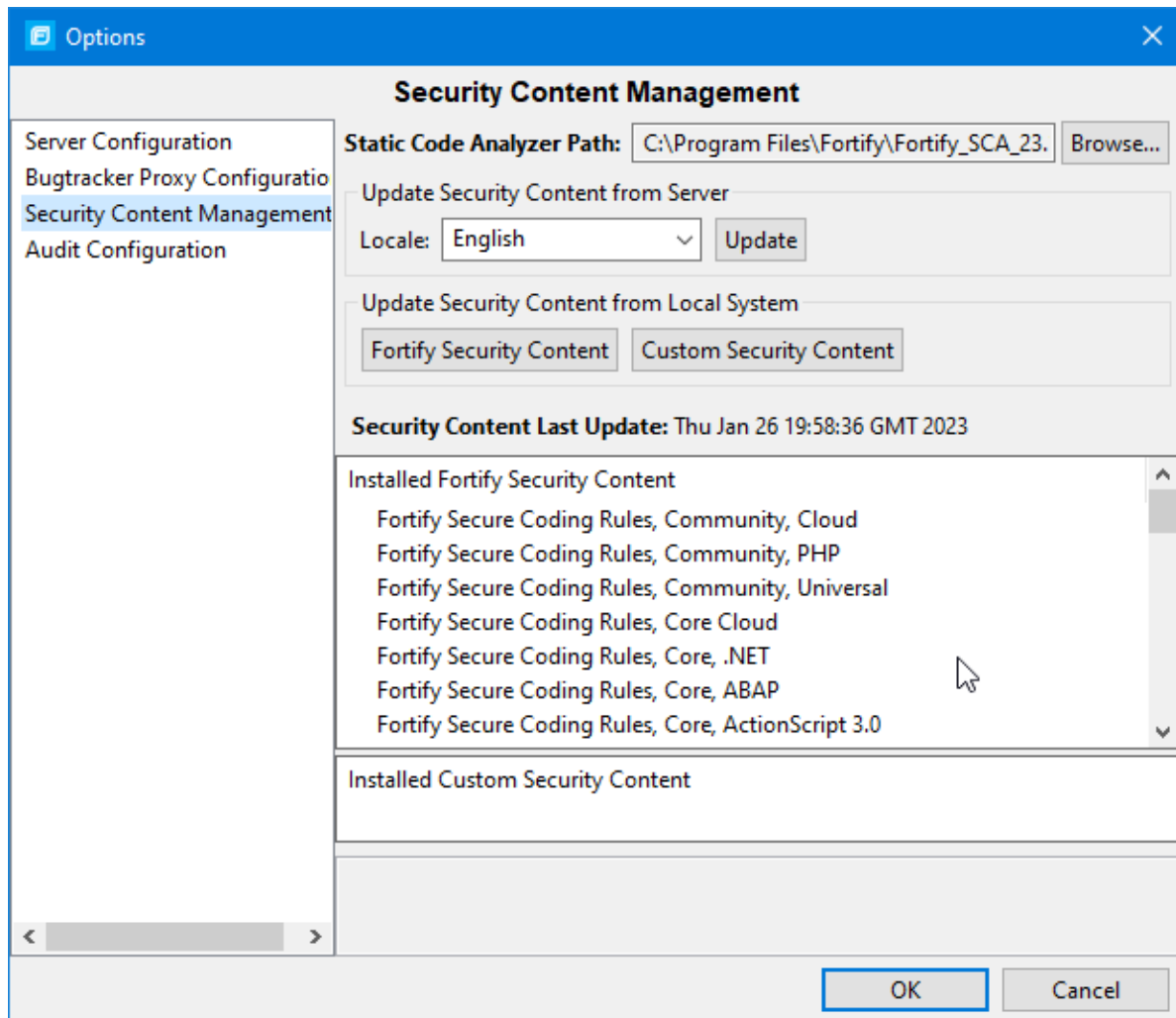
Updating Security Content

To optimize Fortify Audit Workbench 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 **Options > 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 **Static Code Analyzer Path** shows **<Unavailable>**, do the following:
 - a. Click **Browse** to the right of **Static Code Analyzer Path**.
 - b. Go to the Fortify Static Code Analyzer installation directory and select the executable file.
On Windows, the file name is `sourceanalyzer.exe`. On non-Windows systems, the file name is `sourceanalyzer`.
 - c. Click **OK**.

4. To update Fortify security content from a server, do the following:
 - a. (Optional) From the **Locale** list, select a language.
Fortify 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 24](#)

Importing Custom Security Content

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

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 **Options > 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**.

Chapter 3: Scanning Source Code

You can scan your source code and view the analysis results in the Fortify Audit Workbench auditing interface.

This section contains the following topics:

- [Scanning Java Projects](#) 29
- [About Quick Scan Mode](#) 31
- [Scanning Large and Complex Projects](#) 31
- [Scanning Visual Studio Solutions](#) 35
- [Rescanning Projects](#) 37

Scanning Java Projects

The Audit Guide Wizard combines the translation and analysis phases of the scanning process into a single step. Use this wizard to scan small Java projects that have source code in a single directory.

To scan a new Java project:

1. Start Fortify Audit Workbench.
2. Under **Start New Project**, click **Scan Java Project**.
3. Select the folder that contains all the source code you want to analyze, and then click **Select Folder**.

Note: Fortify Static Code Analyzer sets the build ID to the folder name.

4. Select the Java version used for your project, and then click **OK**.

The Audit Guide Wizard opens.

Audit Guide Wizard

How concerned about security are you?

Show me all issues that may have security implications.

Show me likely problems.

Show me only remotely exploitable issues.

I am concerned about attacks that can originate from remote and local attackers. This program might be influenced by data sources that have not been verified for data integrity.

Are you concerned about code quality in addition to security?

Show me all code quality issues.

Show me quality issues that may result in program instability.

No, I don't want to see code quality issues.

I am concerned about issues that may impact stability or make the codebase more difficult to maintain.

Is this a Java EE Web application?

Yes

No

Does this program run with escalated privileges (such as administrator account, root user, account with access to sensitive data, etc.)?

Yes

No

Scan **Cancel**

5. Select the settings for the types of issues you want to display in the results, and then click **Scan**. Fortify Static Code Analyzer analyzes the source code. If Fortify Static Code Analyzer encounters any problems as it scans the source code, Fortify Audit Workbench displays a warning.
6. If a warning is displayed, click **OK**.
7. After the scan is complete, Fortify Audit Workbench displays the analysis results. Fortify Audit Workbench stores the analysis results (FPR file) in the following directory:
 - Windows: C:\Users\\AppData\Local\Fortify\AWB-<version>\<build_ID>
 - Non-Windows: <userhome>/.fortify/AWB-<version>/<build_ID>

Note: Fortify Static Code Analyzer scans started from Fortify Audit Workbench are invoked with the server Java Virtual Machine.

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. Fortify 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*.

To perform a quick scan, follow the steps described in "[Scanning Large and Complex Projects](#)" below and select the **Enable Quick Scan Mode** check box. Quick scan is also available when you scan Visual Studio solutions (see "[Scanning Visual Studio Solutions](#)" on page 35). Fortify Audit Workbench displays the scan results in its **Project Summary** view. You audit quick scan results just as you audit full scan results.

Scanning Large and Complex Projects

Exceptionally large codebases might require some configuration to ensure a complete scan, including using Fortify Static Code Analyzer to scan the code in smaller sections. While Fortify Audit Workbench enables you to edit Fortify Static Code Analyzer command options, you can handle large, complex scans more successfully directly through the command console. In addition, if a system has memory constraints, Fortify Static Code Analyzer must compete with the Fortify Audit Workbench for resources, which might result in slow or failed scans.

Use the Advanced Static Analysis wizard for projects that have source code in multiple directories, special translation or build requirements, or that have files that you want to exclude from the project.

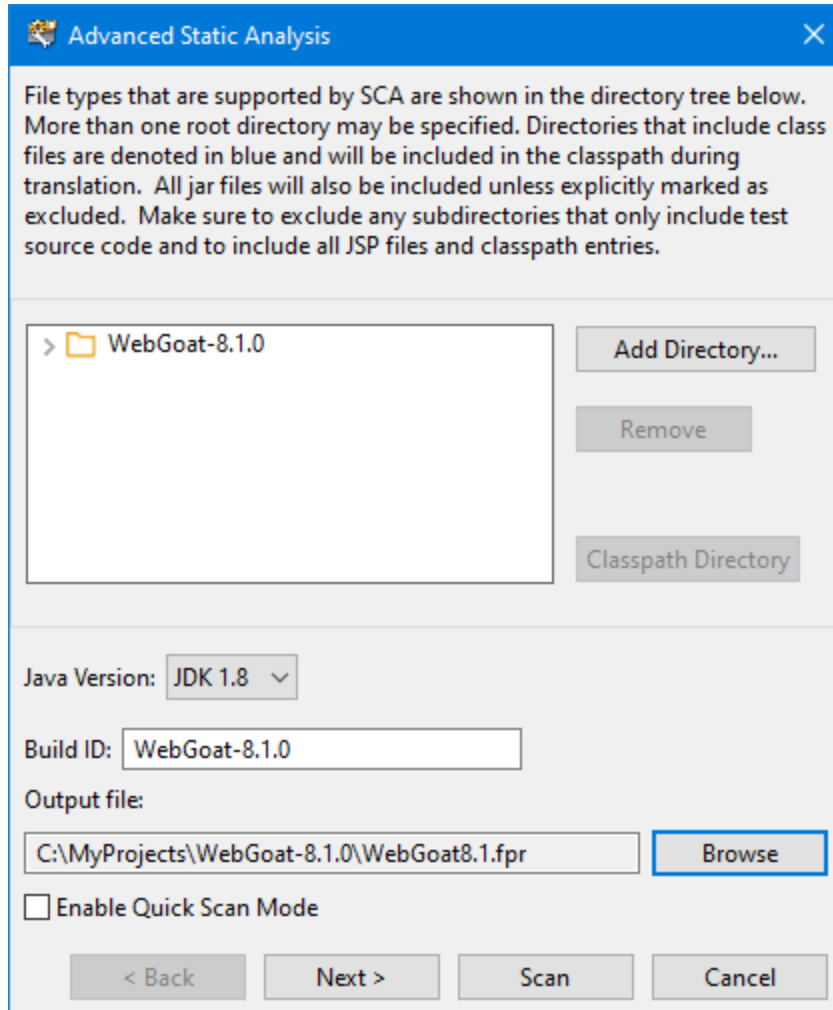
Note: Fortify Audit Workbench filters out unsupported files within the selected source code directories.

To scan a new project:

1. Start Fortify Audit Workbench.
2. Under **Start New Project**, click **Advanced Scan**.
3. Select the root directory of the project, and then click **Select Folder**.

The Advanced Static Analysis wizard opens.

Note: The following image shows the wizard options when you select a Java project. The options are different for other programming languages.



The wizard automatically includes all supported files in the scan.

4. (Optional) To add files from another directory:
 - a. Click **Add Directory**.
 - b. Select the folder that contains the files you want to add to the scan, and then click **Select Folder**.

The navigation pane displays the directory and Fortify Audit Workbench adds all supported files to the scan. (To remove the directory, right-click the folder, and then select **Remove Root**.)
5. (Optional) To exclude files or directories that contain, for example, test source code, right-click the file or directory, and then click **Exclude**.

6. For Java projects, set the following:
 - a. Select the build directories and JAR files, and then click **Classpath Directory**.

Note: If you do not select the classpath directory, Fortify Static Code Analyzer uses the CLASSPATH environment variable value.

The folder turns blue and the files are added to the class path.

- b. From the **Java Version** list, select the Java version of the project.
7. In the **Build ID** box, type a build ID.
The root directory is the default build ID.
8. 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 will generate.
9. 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 31.
10. Click **Next**.

The analysis process includes the following phases:

- During the *clean* phase, Fortify Static Code Analyzer removes files from previous translation of the project.
 - During the *translation* phase, Fortify Static Code Analyzer translates source code identified in the previous page into an intermediate format that is associated with a build ID. The build ID is typically the project.
 - During the *scan* phase, Fortify Static Code Analyzer scans source files identified during the translation phase and generates analysis results, in the Fortify Project Results (FPR) format.
11. (Optional) To skip an analysis phase, clear the **Enable clean**, **Enable translation**, or **Enable scan** check box.
For example, if the security content has changed but the project has not changed, you might want to skip both the clean and the translation phases so that Fortify Static Code Analyzer scans the project without translating it again.
 12. Modify the command-line options for each Fortify Static Code Analyzer analysis phase to suit your requirements.
 13. (Optional) To specify the amount of memory Fortify Static Code Analyzer used for analysis:
 - a. Click **Configure Memory**.
 - b. Adjust the slider to the amount of memory required.

Note: Fortify Audit Workbench displays the amount of memory you set for Fortify Static Code Analyzer followed by the amount of memory on your system.

- c. Click **OK**.

14. (Optional) To analyze the source code using an installed custom Rulepack, or to turn off a Rulepack, do the following:
 - a. Click **Configure Rulepacks**.
The Additional Options dialog box opens.
 - b. In the **Installed Fortify Security Content** list, clear the check boxes that correspond to any Rulepacks you want to make unavailable during the scan.

Note: For instructions on how to add custom security content, see ["Importing Custom Security Content"](#) on page 28.

- c. Click **OK**.
15. From the Advanced Static Analysis wizard, click **Next**.

Advanced Static Analysis

How concerned about security are you?

Show me all issues that may have security implications.

Show me likely problems.

Show me only remotely exploitable issues.

I am concerned about attacks that can originate from remote and local attackers. This program might be influenced by data sources that have not been verified for data integrity.

Are you concerned about code quality in addition to security?

Show me all code quality issues.

Show me quality issues that may result in program instability.

No, I don't want to see code quality issues.

I am concerned about issues that may impact stability or make the codebase more difficult to maintain.

Is this a Java EE Web application?

Yes

No

Does this program run with escalated privileges (such as administrator account, root user, account with access to sensitive data, etc.)?

Yes

No

< Back Next > Scan Cancel

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

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

After the scan is complete, Fortify Audit Workbench loads the audit project and displays the analysis results.

Scanning Visual Studio Solutions

If you have Visual Studio and the Fortify Extension for Visual Studio installed on the same machine as Fortify Audit Workbench, you can analyze Visual Studio solutions and projects.

To scan a Visual Studio solution:

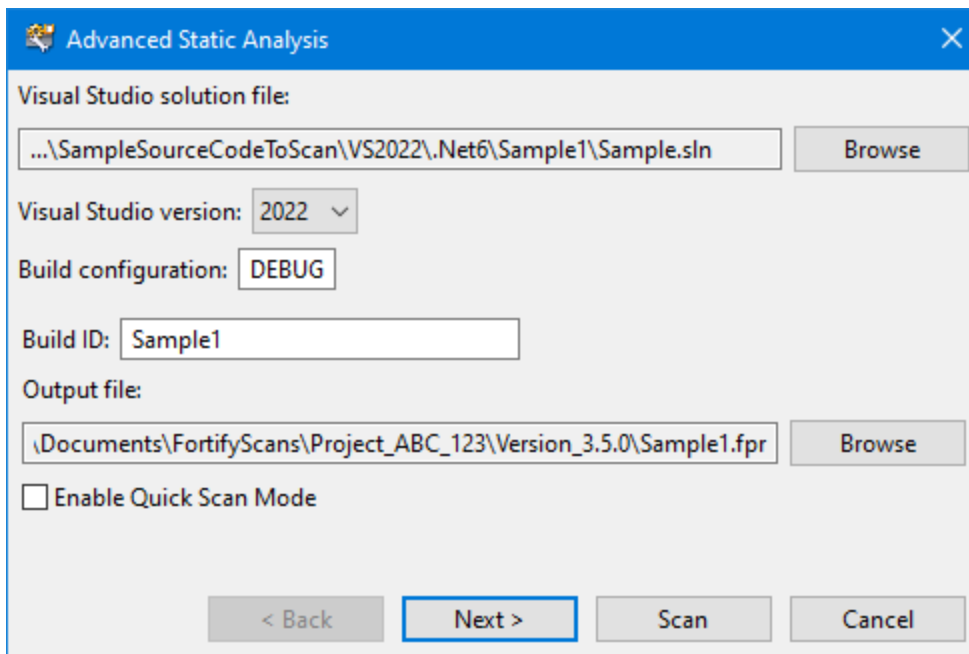
1. Start Fortify Audit Workbench.
2. Under **Start New Project**, click **Visual Studio Build Integration**.

Note: The **Visual Studio Build Integration** command is only available if you have installed the Fortify Extension for Visual Studio with the Fortify Applications and Tools installation.

3. Select the folder that contains the solution you want to analyze, and then click **Select Folder**.

Note: Fortify Static Code Analyzer uses the selected folder name as the build ID.

The Advanced Static Analysis wizard opens.



The screenshot shows the 'Advanced Static Analysis' dialog box. It has a blue title bar with the Fortify logo and the text 'Advanced Static Analysis'. The dialog contains the following fields and controls:

- Visual Studio solution file:** A text box containing the path '...\SampleSourceCodeToScan\VS2022\.Net6\Sample1\Sample.sln' and a 'Browse' button to its right.
- Visual Studio version:** A dropdown menu showing '2022'.
- Build configuration:** A text box containing 'DEBUG'.
- Build ID:** A text box containing 'Sample1'.
- Output file:** A text box containing the path '\Documents\FortifyScans\Project_ABC_123\Version_3.5.0\Sample1.fpr' and a 'Browse' button to its right.
- Enable Quick Scan Mode:** An unchecked checkbox.
- Navigation buttons:** At the bottom, there are four buttons: '< Back', 'Next >', 'Scan', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

4. Configure the solution settings as follows:
 - a. (Optional) Next to the **Visual Studio solution file** box, click **Browse**. Navigate to and select your Visual Studio solution file.
 - b. From the **Visual Studio version** list, select the Visual Studio version used for the solution.
 - c. In the **Build configuration** box, leave the default value DEBUG.
 - d. (Optional) In the **Build ID** box, type a different build ID.

- e. (Optional) To change the output location and file name, click **Browse** to the right of **Output file**.
- f. To run the scan in quick scan mode, select the **Enable Quick Scan Mode** check box.
- g. Click **Next**.

The Advanced Static Analysis wizard displays details about the Fortify Static Code Analyzer analysis phases for the scan.

- During the *clean* phase, Fortify Static Code Analyzer removes files from previous translation of the project.
 - During the *translation* phase, Fortify Static Code Analyzer translates source code identified in the previous page into an intermediate format that is associated with a build ID. The build ID is typically the project.
 - During the *scan* phase, Fortify Static Code Analyzer scans source files identified during the translation phase and generates analysis results, in the Fortify Project Results (FPR) format.
5. (Optional) To skip a scanning phase, clear the **Enable clean**, **Enable translation**, or **Enable scan** check box.
For example, if the Rulepacks have changed but the project has not changed, you might want to skip both the clean and the translation phases so that Fortify Static Code Analyzer scans the project without retranslating the source code.
 6. Modify the command-line options for each Fortify Static Code Analyzer phase, if necessary.
 7. (Optional) To specify the amount of memory Fortify Static Code Analyzer uses for scanning:
 - a. Click **Configure Memory**.
 - b. Adjust the slider to the amount of memory required.

Note: Fortify Audit Workbench displays the amount of memory you set for Fortify Static Code Analyzer followed by the amount of memory on your system.

- c. Click **OK**.
8. (Optional) To analyze the source code using an installed custom Rulepack, or to turn off a Rulepack, do the following:
 - a. Click **Configure Rulepacks**.
 - b. In the **Installed Fortify Security Content** list, clear the check boxes that correspond to any Rulepacks you want to make unavailable during the scan.

Note: For instructions on how to add custom security content, see "[Importing Custom Security Content](#)" on page 28.

- c. Click **OK**.
9. From the Advanced Static Analysis wizard, click **Next**.
10. Select your scan settings, and then click **Scan**.

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

After the scan is completed, Fortify Audit Workbench loads the audit project and displays the analysis results.

Rescanning Projects

This section describes how to rescan a project that was translated locally with new or updated rules. Fortify Audit Workbench automatically loads the FPR project settings such as the build ID and source code path, and allows you to change the command-line scanning options.

After Fortify Static Code Analyzer completes the scan, Fortify Audit Workbench merges the analysis results with those from the previous scan to determine which issues are new, which have been removed, and which were uncovered in both scans.

To rescan a project:

1. Open an FPR file.
2. Select **Tools > Rescan Project**.

Note: You can only rescan a project on the same machine where the project was originally scanned.

The Rescan Build ID dialog box opens.

3. If the source code has changed since the most recent scan, click **Update Project Translation** to re-translate the project.

Note: If the FPR file that you opened was generated by a Fortify Static Code Analyzer scan that was not initiated from Fortify Audit Workbench, then **Update Project Translation** is unavailable.

Note: If the source code has changed since the most recent scan, you must update the translation before you rescan the code. Otherwise, a new scan cannot uncover the issues in the updated source code.

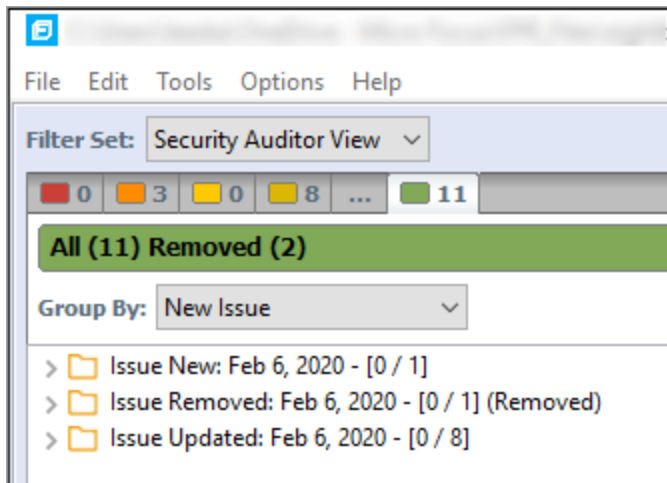
4. (Optional) Modify the Fortify Static Code Analyzer scan phase command-line options, as necessary.
5. To perform a quick scan, select the **Enable Quick Scan Mode** check box.
6. (Optional) To change the Rulepacks used to analyze the project:
 - a. Click **Configure Rulepacks**.
 - b. Click to expand the **Installed Fortify Security Content**.
 - c. To add and remove Rulepacks, select or clear the check boxes, as necessary.

Note: For instructions on how to add custom security content, see ["Importing Custom Security Content" on page 28](#).

- d. Click **OK**.
7. Click **Scan**.

After the scan is complete, Fortify Audit Workbench displays the results. Compare the new results with the issues uncovered in the previous scan as follows:

- To display all new issues, select the **All** tab (green), and then, in the **Group By** list, select **New Issue**. Expand the **Issue New** group.
- To display removed issues, select the **All** tab, and then select **Options > Show Removed Issues**.
- To review issues found in both the previous scan and the new scan, select the **All** tab, and then in the **Group By** list, select **New Issue**. Expand the **Issue Updated** group.



Chapter 4: Viewing Analysis Results

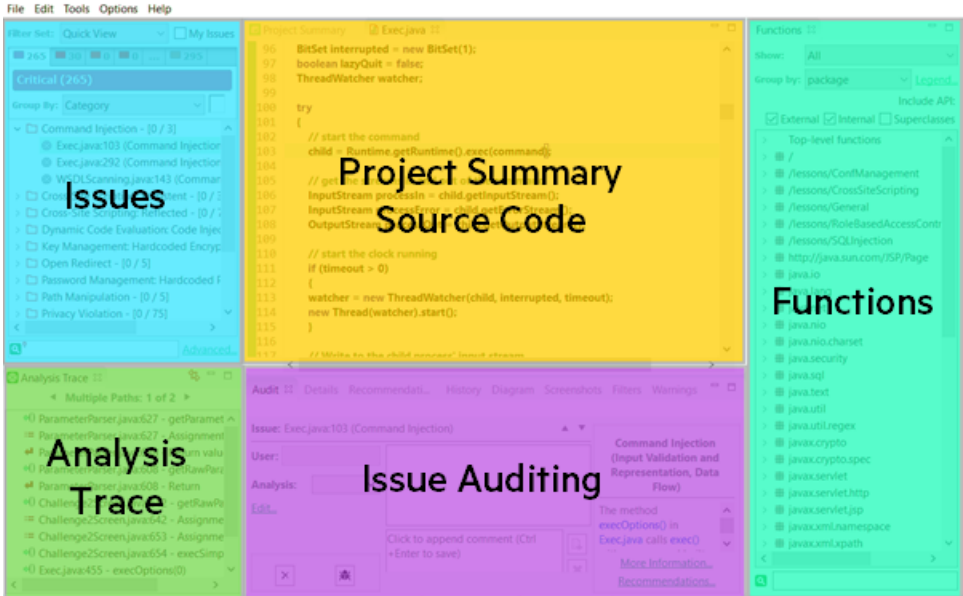
After a scan is completed, Fortify Audit Workbench displays the analysis results in the auditing interface.

This section contains the following topics:

- About Viewing Analysis Results 39
- Searching for Issues 61
- Working with Issues 72
- About Issue Templates 82
- Configuring Custom Filter Sets and Filters 83
- Managing Folders 87
- Configuring Custom Tags for Auditing 91
- Issue Template Sharing 95
- Advanced Configuration 98

About Viewing Analysis Results

After the scan is complete (or, after you open an existing audit project), summary analysis results are displayed in the **Issues** view and in the **Project Summary** view of the auditing interface. The **Analysis Trace** and **Issue Auditing** views are open, but do not contain any information until you select an issue from the **Issues** view.

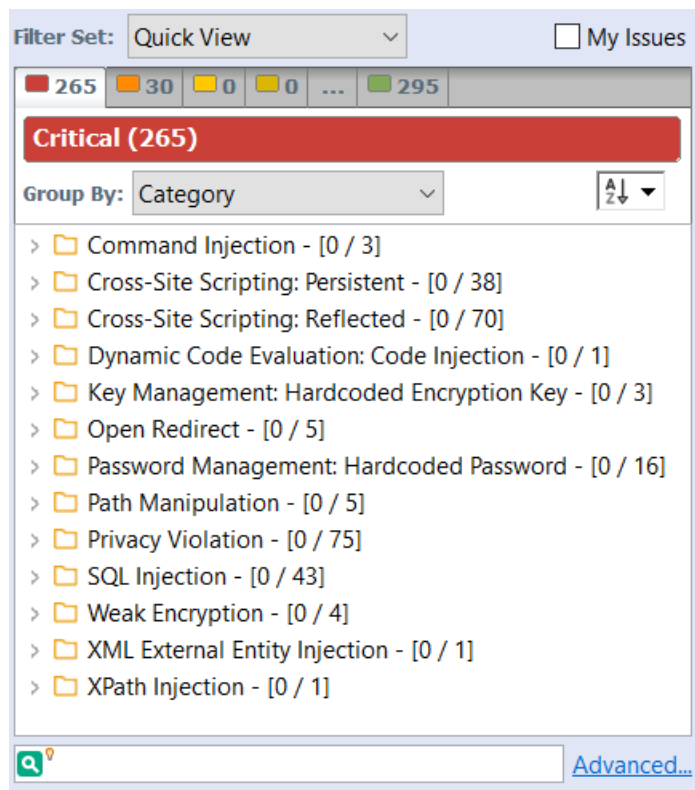


View / Tab	More Information
Issues (top left)	"Issues View" below
Project Summary (top center)	"Project Summary View" on page 45
Source Code (top center)	"Source Code Tab" on page 49
Analysis Trace (bottom left)	"Analysis Trace View" on page 50
Issue Auditing (bottom center)	"Issue Auditing View" on page 52
Functions (right)	"Functions View" on page 59

Issues View

The **Issues** 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

Fortify Audit Workbench applies filters to sort and display the issues that Static Code Analyzer uncovers. Fortify Audit Workbench organizes filters into distinct *filter sets*.

The selected filter set controls which issues are listed in the **Issues** 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.

Fortify Audit Workbench 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 83](#).

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 Audit Workbench 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:

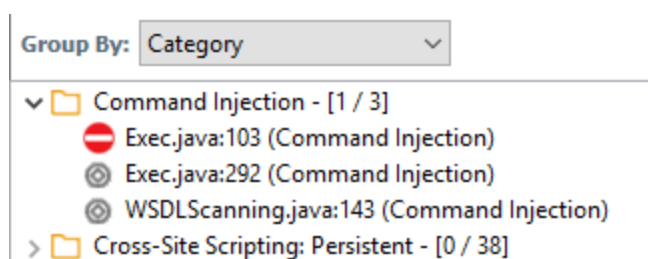
1. Select **Options > Options**.
2. In the left pane, select **Audit Configuration**, and then select the **Configuration** tab on the right.
3. Under **Audit Project Load Mode**, leave the **Default Filter Set** check box selected.
If you clear the check box, the default filter is loaded. For newly-opened 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 **Issues** 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 Audit Workbench, the term folder *does not* refer to the folder icon 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.

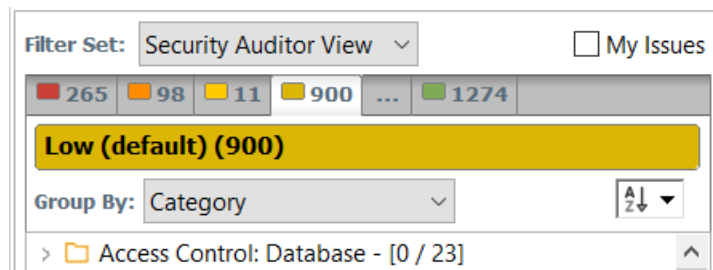


The filter set you select from the **Filter Set** list determines which folders are visible in the Issues view. The following table describes the folders that are visible when the **Security Auditor View** filter set is selected.

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.

Folder	Description
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 Issues View" on page 59](#)).

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 73](#)

["Creating a Custom Grouping Option" on page 76](#)

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 **Options > 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 Issues View. Select a sort option from the **Sort** list. The following table describes the sort options.

Sort Method	Icon	Description
Alphabetical		Sorts the groups and the issues within the groups in alphabetical order
		Sorts the groups and the issues within the groups in reverse-alphabetical order
Group size		Sorts the groups by the number of contained issues from largest to smallest
		Sorts the groups by the number of contained issues from smallest to largest
Last modified date		Sorts the groups and issues in groups by the date last modified by 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 62](#).

Project Summary View

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

To open this view, select **Tools > 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 57](#).

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
- 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

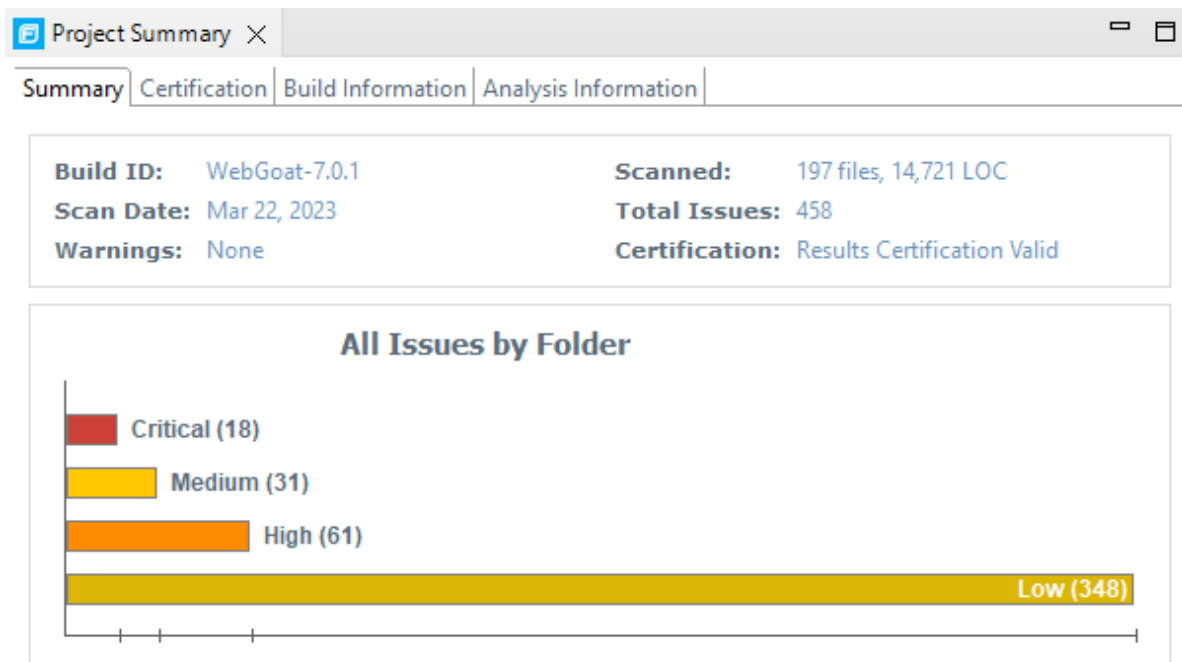
The summary graph displayed in the **Project Summary** view provides multiple perspectives on the sets of issues, grouped by priority (Critical, High, Medium, and Low) uncovered in a scan. You can drill down in the graph to see detailed information about each issue set, and create various bar charts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

To access details about issue sets in an audit project:

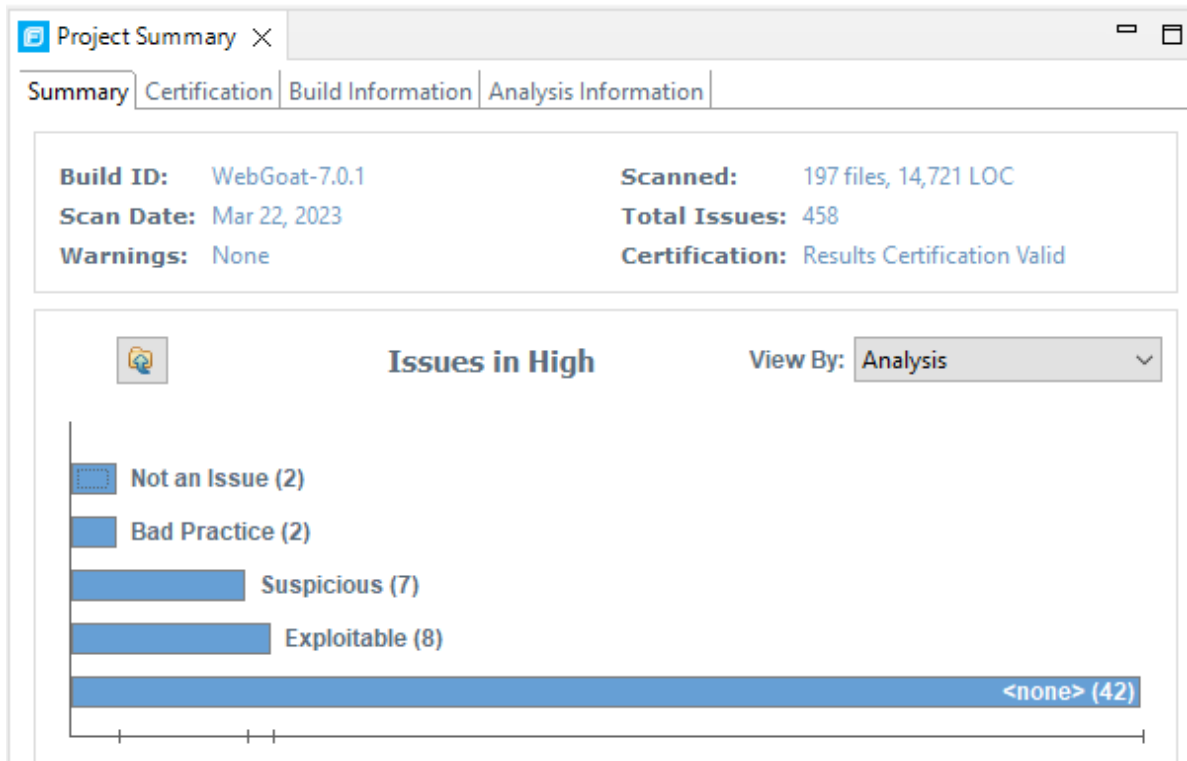
1. Scan your project source code or open an existing audit project.

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 (**Issues**), the summary graph changes accordingly.



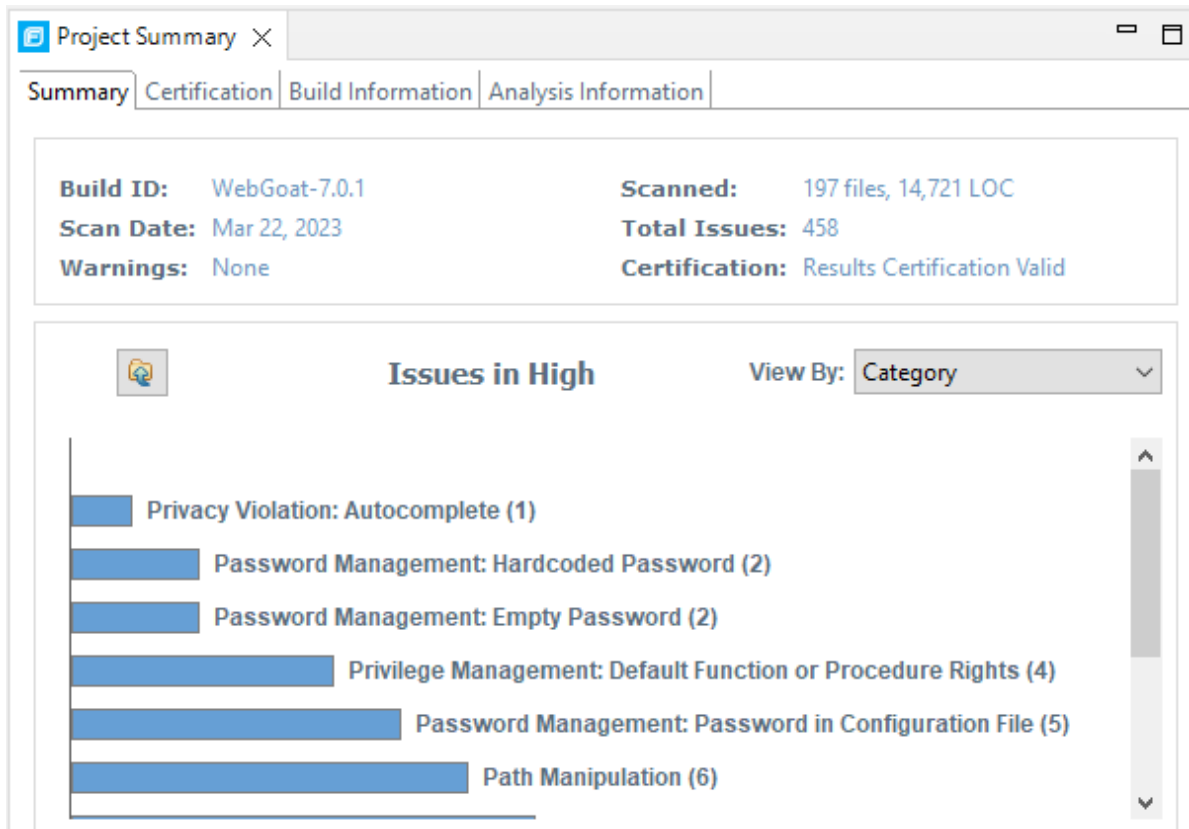
2. To see a different view of the high priority issues, click the **High** bar.



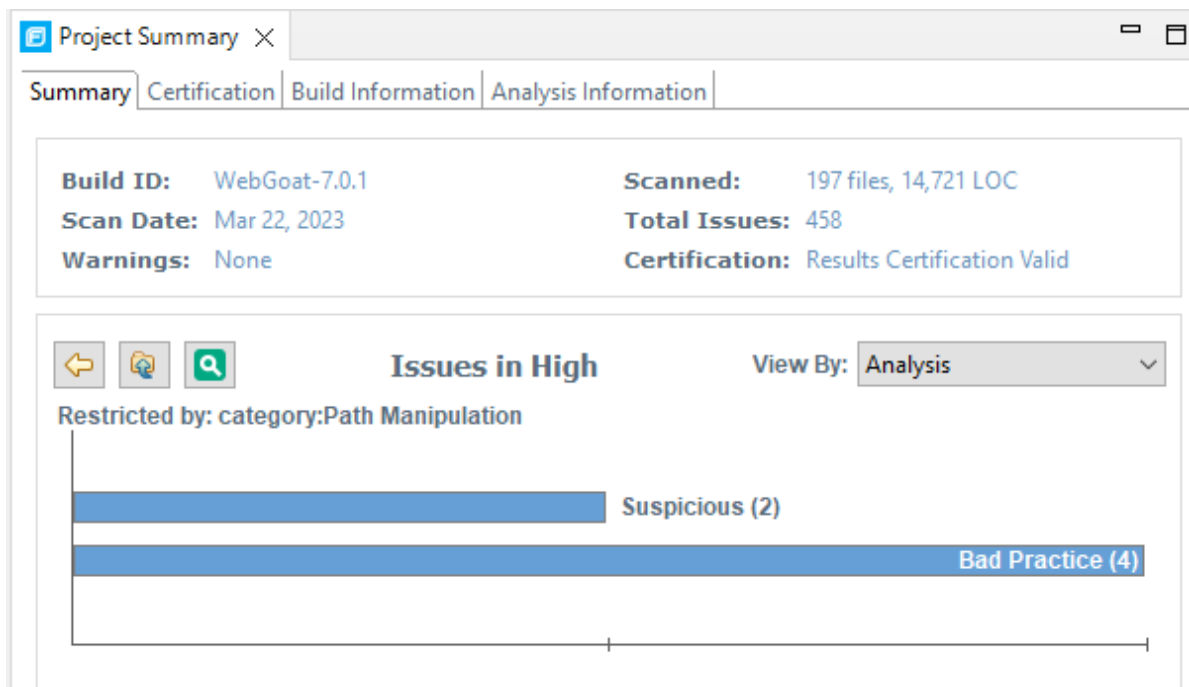
By default, the graph displays high priority issues based on the analysis attribute (assigned analysis values).

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.

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

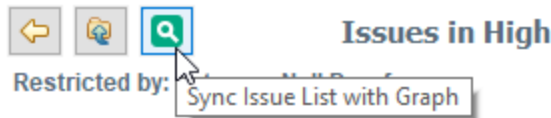


- On the **Issues in High** bar graph, select a bar for a category that contains multiple issues.

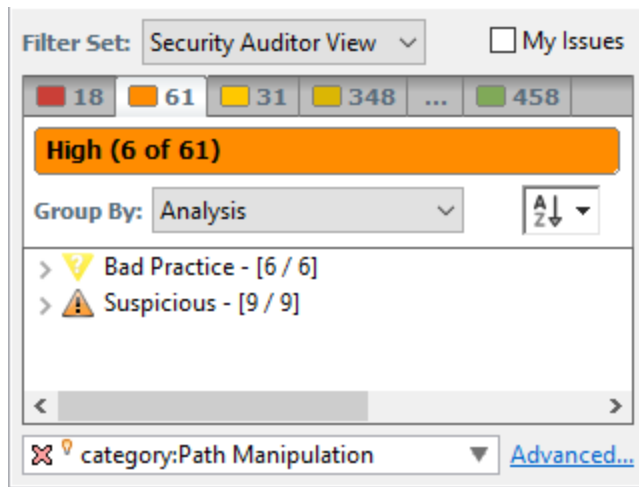


In the example shown here, the **Path Manipulation** bar is selected. You can see that of the six issues, two are marked as Suspicious and four are marked as Bad Practice.

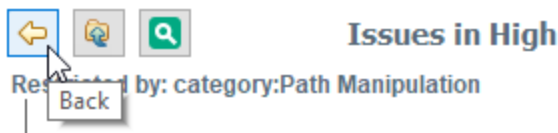
5. To synchronize the issues list with the displayed graphical view, click **Sync Issue List with Graph**.



The issue list in the **Issues** view now reflects the selections in the summary graph.



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



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



Source Code Tab

After you open a project in Fortify Audit Workbench, the top center view displays the **Project Summary** tab. After you select an issue in the **Issues** view to the left, Fortify Audit Workbench adds the source code tab to the top center view. This source code tab shows the code related to the issue selected in the **Issues** view.

If multiple nodes represent an issue in the **Analysis Trace** view (below the **Issues** view), the source code tab shows the code associated with the selected node.

From the source code tab, you can use the context menu commands to:

- Create new issues (**Create New Issue**).
For more information, see ["Creating Issues for Undetected Vulnerabilities" on page 107](#).
- Create a custom rule (**Generate Rule for Function**).
For more information, see ["Writing Rules for Functions" on page 133](#).
- Jump to the declaration of a function, class, variable, field, or an argument within source code that Fortify Static Code Analyzer translated (**Jump to Declaration**).
- Locate the file name and line number where a function occurs in the source code (**Find Usages**).
The search results are displayed in the **Search** tab of the **Issue Auditing** view.
- Refresh the code displayed in source code tab (**Refresh**).
You might need to use this if the file was modified outside of Fortify Audit Workbench.
- Customize the appearance in the source code tab such as fonts, colors, text edit settings, and so on (**Editor Preferences**).

About Displayed Source Code

After you open an FPR file in Audit Workbench, the source code tab displays source code that is stored locally. If that source code was updated since the last scan, Fortify Audit Workbench displays the updated source code, even if the latest scan did not use that updated source code.



However, if that source code is updated after you open the FPR file and Fortify Audit Workbench has already started and searched for the source code (even if you close the FPR in Audit Workbench and then re-open it) Fortify Audit Workbench does not look for or display the updated source code. It displays the updated source code only after you quit, and then restart Fortify Audit Workbench.

















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.

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

The **Analysis Trace** view uses the icons described in the following table to show how the dataflow moves in this section of the source code or execution order.

Icon	Description
	Data is assigned to a field or variable
	Information is read from a source external to the code such as an HTML form or a web address

Icon	Description
	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
	<p>Passthrough, tainted data passes from one place to another</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Note: This is typically shown as <code>functionA(x : y)</code> to indicate that data is transferred from <code>x</code> to <code>y</code>. The <code>x</code> and <code>y</code> values are one of the following:</p> <ul style="list-style-type: none"> • An argument index • <code>return</code>—The return value of a function • <code>this</code>—The instance of the current object • A specific object field or key </div>
	An alias is created for a memory location
	Data is read from a variable
	Data is read from a global variable
	Tainted data is returned from a function
	A pointer is created
	A pointer is dereferenced
	The scope of a variable ends
	The execution jumps
	A branch is taken in the code execution
	A branch is not taken in the code execution
	Generic

Icon	Description
	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:

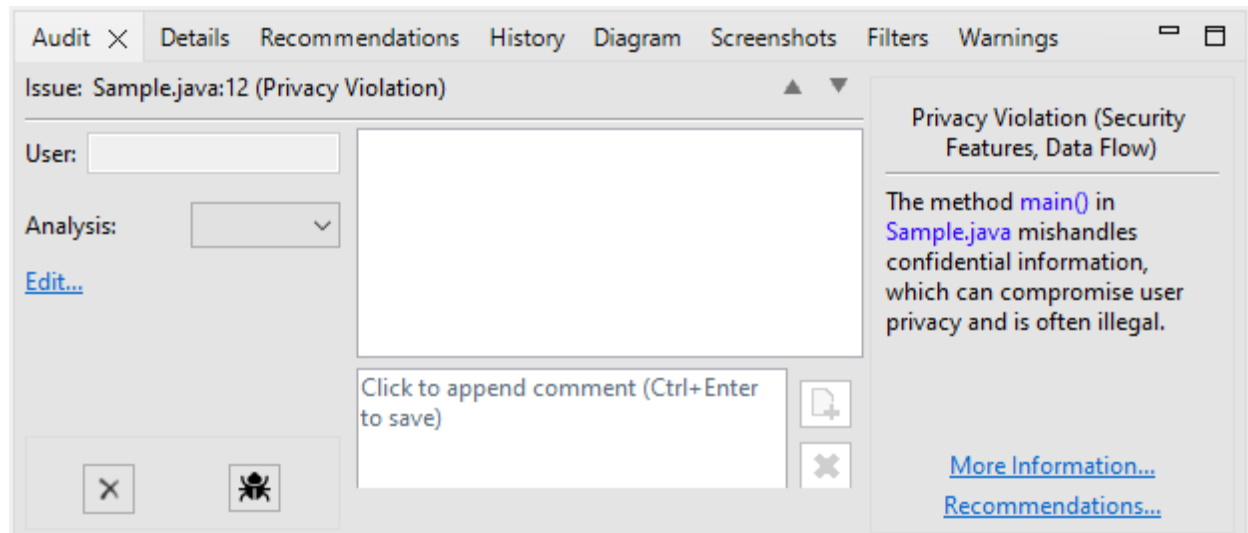
- A text node, displayed in italics as a child of the trace node. This text node is expanded by default.
- An induction trace, displayed as a child of the text node (a box surrounds the induction trace).

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 auditing interface 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 **Options > 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>	<p>Displays any custom tags if defined for the audit project. These are displayed below the primary tag.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>For more information about Fortify Audit Assistant, see the <i>OpenText™ Fortify Software Security Center User Guide</i>.</p>
 Suppress	Suppresses the issue.
 Unsuppress	Unsuppresses the issue (only visible if the issue is suppressed). Suppressed issues are hidden by default. To display suppressed issues, select Options > Show Suppressed Issues .

Element	Description
 File Bug	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.

Note: For more information about metadata values, see ["Estimating Impact and Likelihood with Input from Rules and Analysis" on page 142](#).

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.

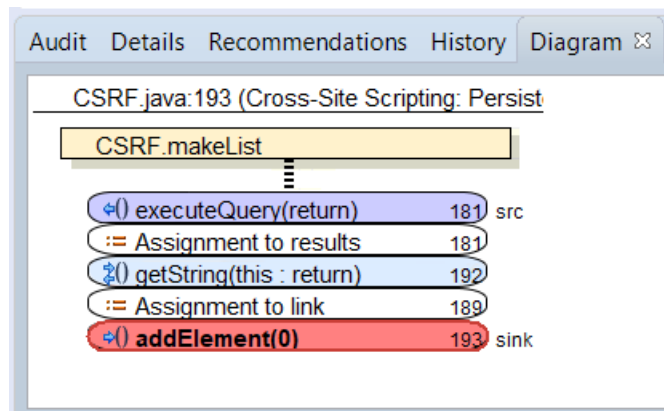
Section	Description
Recommendations/Custom Recommendations	Describes possible solutions for the selected issue. It can also include examples and recommendations defined by your organization.
Tips/Custom Tips	Provides useful information specific to the selected issue, and any custom tips defined by your 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 **Issues** view. This tab displays information that is relevant to the rule type. The vertical axis represents the execution order.



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

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

The icons used for the expression type of each node in the diagram are the same icons used in the **Analysis Trace** view. For a description of the icons, see ["Analysis Trace View" on page 50](#).

Filters Tab

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

The screenshot shows the 'Filters' tab in the application. The 'Quick View Filters' section is active, showing the following filters:

- Visibility Filters**
 - If impact is not in range [2.5, 5.0] Then hide issue
 - If likelihood is not in range (1.0, 5.0) Then hide issue
- Folder Filters**
 - If [fortify priority order] contains critical Then set folder to Critical
 - If [fortify priority order] contains high Then set folder to High
 - If [fortify priority order] contains medium Then set folder to Medium
 - If [fortify priority order] contains low Then set folder to Low

On the right side, there are several action buttons: Show Matching Issues, Disable Filter, Edit Filter..., Create New Filter..., Delete Filter, Copy Filter, and Copy Filter To...

The following table describes the options to create new filters.

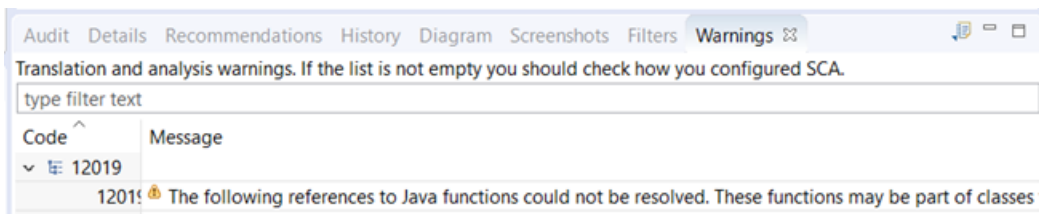
Option	Description
Filters	<p>Displays a list of the visibility and folder filters configured in the selected filter set where:</p> <ul style="list-style-type: none">• Visibility filters show or hide issues• Folder filters sort the issues into the folder tabs in the Issues view <p>Right-click a filter to show issues that match the filter or to enable, disable, copy, or delete it.</p>
If	<p>Displays conditions for the selected filter.</p> <p>The first list displays issue attributes, the second specifies how to match the attribute, and third is the value the filter matches.</p> <p>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.</p>
Then	<p>Indicates the filter type, where Hide Issue is a visibility filter and Set Folder to is a folder filter.</p> <p>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.</p>

See Also

["Creating a Filter from the Issue Auditing View" on page 85.](#)

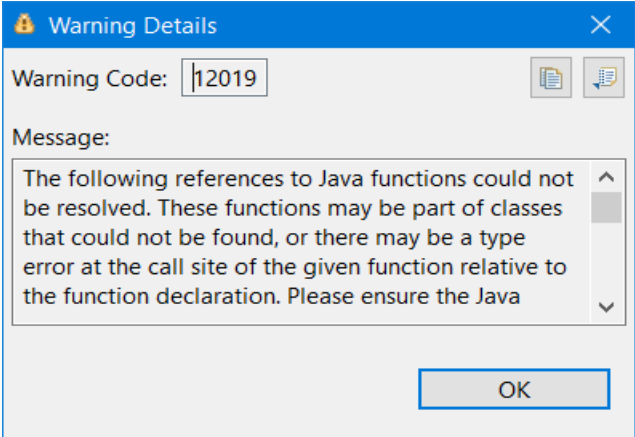

Warnings Tab

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.	<ul style="list-style-type: none"> Double-click the message. 
Copy a warning message to the clipboard.	<ul style="list-style-type: none"> Right-click a message, and then select Copy.
Save a warning message to a file.	<ol style="list-style-type: none"> Right-click a message, and then select Export Entry. Type a name for the file, and then click Save. <p>The file includes the audit project name, FPR file location, the warning code, and the warning message.</p>
Save all the warning messages to a file.	<ol style="list-style-type: none"> Click Export Warnings . Type a name for the file, and then click Save. <p>The file includes the project name, FPR file location, the warning codes, and the warning messages.</p>
Search the warning message	Type the search text in the filter text box.

Task	Procedure
<p>Modify the text message at the top of the tab.</p>	<ol style="list-style-type: none"> Edit the <code><fortify_working_dir>/config/tools/warnings-view.properties</code> file where <code><fortify_working_dir></code> is: <ul style="list-style-type: none"> Windows: C:\Users\<code><username></code>\AppData\Local\Fortify Non-Windows: <code><userhome>/ .fortify</code> Edit the text following <code>message=</code> to the text you want to display in the Warnings tab. <p>Close and reopen the Warnings tab to see the updated text.</p>

Functions View

The **Functions** view in the top right shows how and where a function occurs in the source code, whether a security rule covers the function, and which rule IDs match the function. The **Functions** view can also list the functions that Fortify Static Code Analyzer identified as tainted source, and the functions that were not covered by rules in the last scan. For detailed information about the **Functions** view, see ["Using the Functions View" on page 129](#).

Customizing the Issues View

You can customize the **Issues** view to determine which issues it displays.

To change the **Issues** view:

- Select **Options > Options**.
- In the left pane, select **Audit Configuration**.
- 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 Issues view. When multiple scans are run on a project over time, vulnerabilities are often remediated or become obsolete. Fortify Static Code Analyzer marks these vulnerabilities as Removed Issues.

Preference	Description
Show Hidden Issues	Displays all hidden issues.
Collapse Issues	Shows similar issues based on certain attributes under a shared parent node in the Issues view.
Use Short File Names	References the issues in the Issues view by file name only, instead of by relative path.
Show Category of Issue	Displays the category of an issue in the Issues 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.
Parent Fill Opacity	Controls the opacity of the parent tile in Smart View. The setting ranges from 0% opaque on the left to 100% opaque on the right.

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

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:

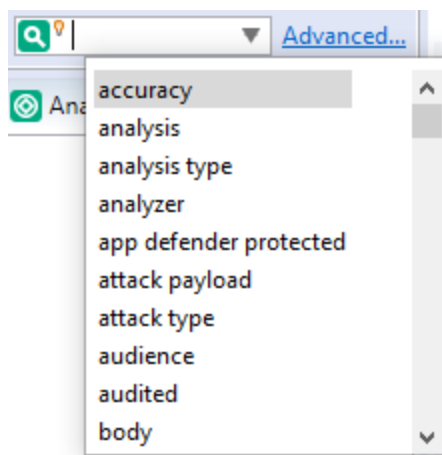
- Type a search query in the search box and press **Enter**.



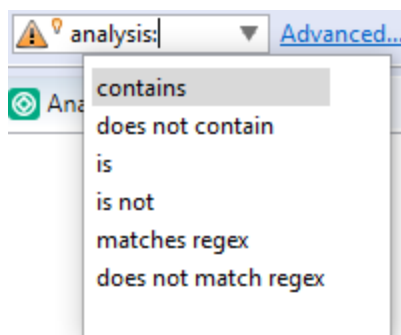
- To select a search query that you used before, click the arrow in the search box, and then select a search query from the list.

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 **Issues** 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 icon in the search box changes to a warning icon 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 70](#).

See Also

["Search Syntax" below](#)

["Search Modifiers" on the next page](#)

["Search Query Examples" on page 70](#)

["Performing Advanced Searches" on page 70](#)

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 70](#)

["Searching for Issues" on page 61](#)

["Performing Advanced Searches" on page 70](#)

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 <code>exploitable</code> , <code>not an issue</code> , 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	<p>Searches for issues based on intended audience such as dev, targeted, medium, broad, and so on.</p> <p>Note: This metadata is legacy information that is no longer used and will be removed in a future release. Fortify recommends that you do not use this search modifier.</p>
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	<p>Searches for issues that contain the search term in the information for the filed bug.</p> <p>Note: This information is discarded each time you restart Fortify Audit Workbench.</p>
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>	<p>Searches for issues based on the value of the specified custom tag.</p> <p>You can search a list-type custom tag using a range of values. The values of a list-type custom tag are an enumerated list where the first value is 0, the second is 1, and so on. You can use the search syntax for a range of numbers to search for ranges of list-type custom tag values. For example, <code>analysis:[0, 2]</code> returns the issues that have the values of the first three analysis values, 0, 1, and 2 (Not an Issue, Reliability Issue, and Bad Practice).</p> <p>To search for a specific date in a date-type custom tag, specify the date in the format: <code>yyyy-mm-dd</code>.</p> <p>To search for issues that have no value set for a custom tag, use <code><none></code> for the search term. For example, to search for all issues that have no value set in the custom tag labeled Target</p>

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 69 .
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 66 .
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 66 .
sourceline	Searches for dataflow issues having taint source entering the flow on the specified line. See also "line" on page 67 .
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.

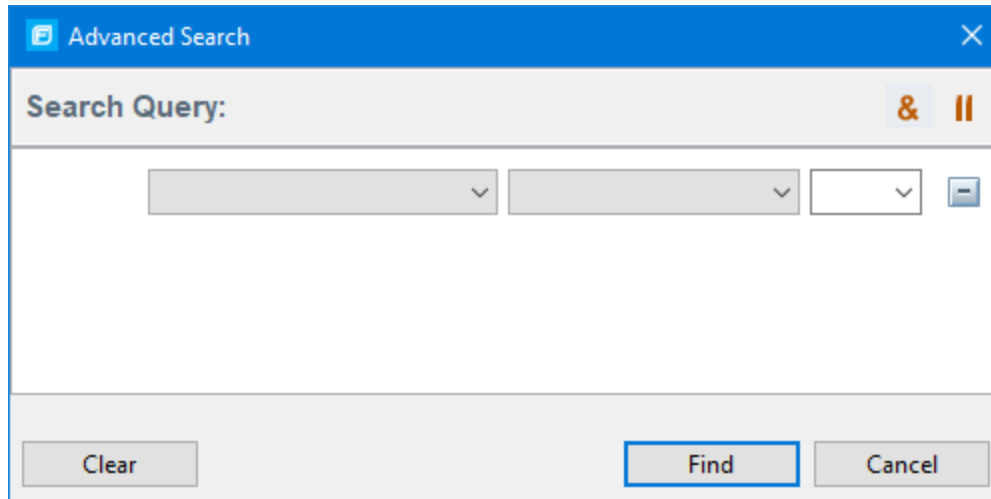
Search Target	Query
All privacy violations in file names that contain jsp with getSSN() as a source	category:privacy violation source:getssn file:jsp
All file names that contain com/test/123	file:com/test/123
All paths that contain traces with mydbcode.sqlcleanse as part of the name	trace:mydbcode.sqlcleanse
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 **AND** (&).
 - To add an OR query row, in the top right corner of the dialog box, click **OR** (||).
4. Add as many query rows as you need for the search query.
5. To delete a row, to the right of the row, click **Delete** (-). 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.

Working with Issues

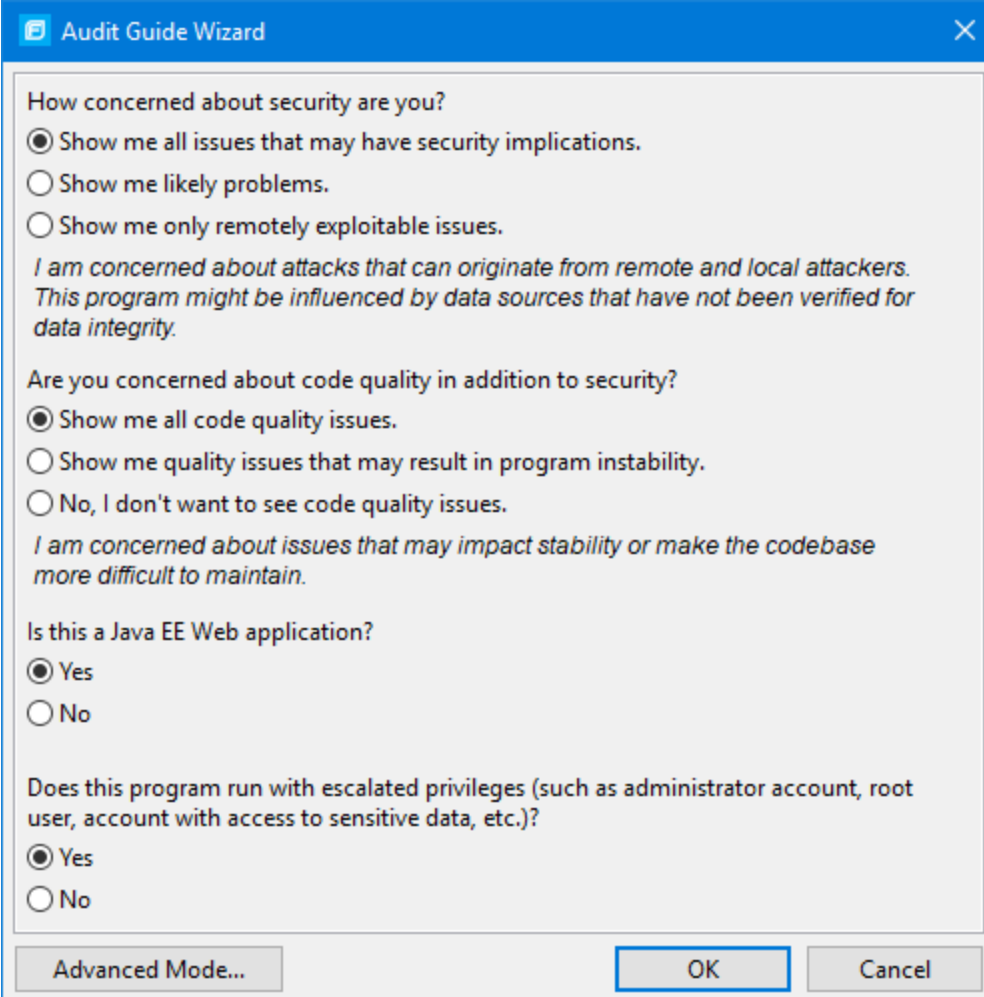
This section describes how to use Audit Workbench to review issues.

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 **Tools > Audit Guide**.



The screenshot shows the 'Audit Guide Wizard' dialog box with the following content:

Audit Guide Wizard [Close]

How concerned about security are you?

- Show me all issues that may have security implications.
- Show me likely problems.
- Show me only remotely exploitable issues.

I am concerned about attacks that can originate from remote and local attackers. This program might be influenced by data sources that have not been verified for data integrity.

Are you concerned about code quality in addition to security?

- Show me all code quality issues.
- Show me quality issues that may result in program instability.
- No, I don't want to see code quality issues.

I am concerned about issues that may impact stability or make the codebase more difficult to maintain.

Is this a Java EE Web application?

- Yes
- No

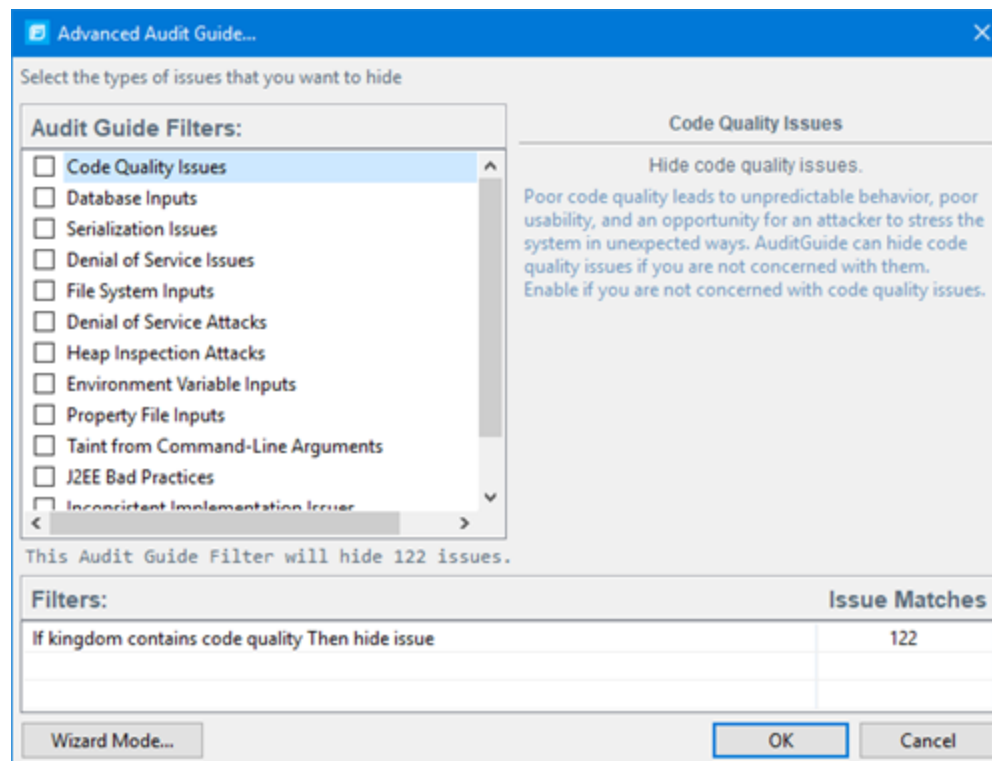
Does this program run with escalated privileges (such as administrator account, root user, account with access to sensitive data, etc.)?

- Yes
- No

Advanced Mode... [OK] [Cancel]

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 **Issues** 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
Shared Trace Node	Groups issues by the most common paths determined by the Dataflow Analyzer. This grouping helps to maximize the number of issues that you can address by updating one location in the code.
Sink	Groups issues that share the same dataflow sink function.
SmartView	Groups issues with a multiple-level grouping based on the last setting applied in SmartView. By default, groups issues by category, and then by Shared Trace Nodes.
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: <code>html</code> , <code>htm</code> , and <code>xhtml</code> are grouped under <code>html</code>).
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.

Option	Description
Status	Groups issues by the audit status (Reviewed , Unreviewed , or Under Review)
URL	Groups dynamic issues by the request web address.

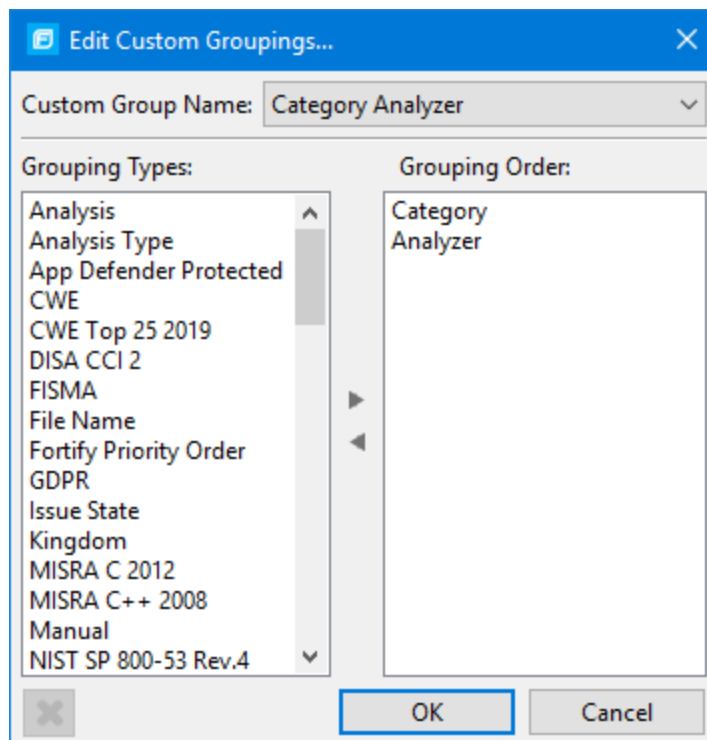
Creating a Custom Grouping Option

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**.

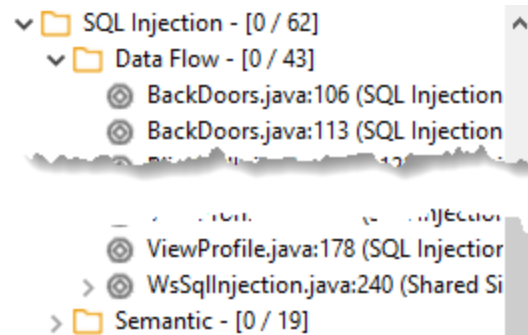
The Edit Custom Groupings dialog box opens.




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 **Delete** .

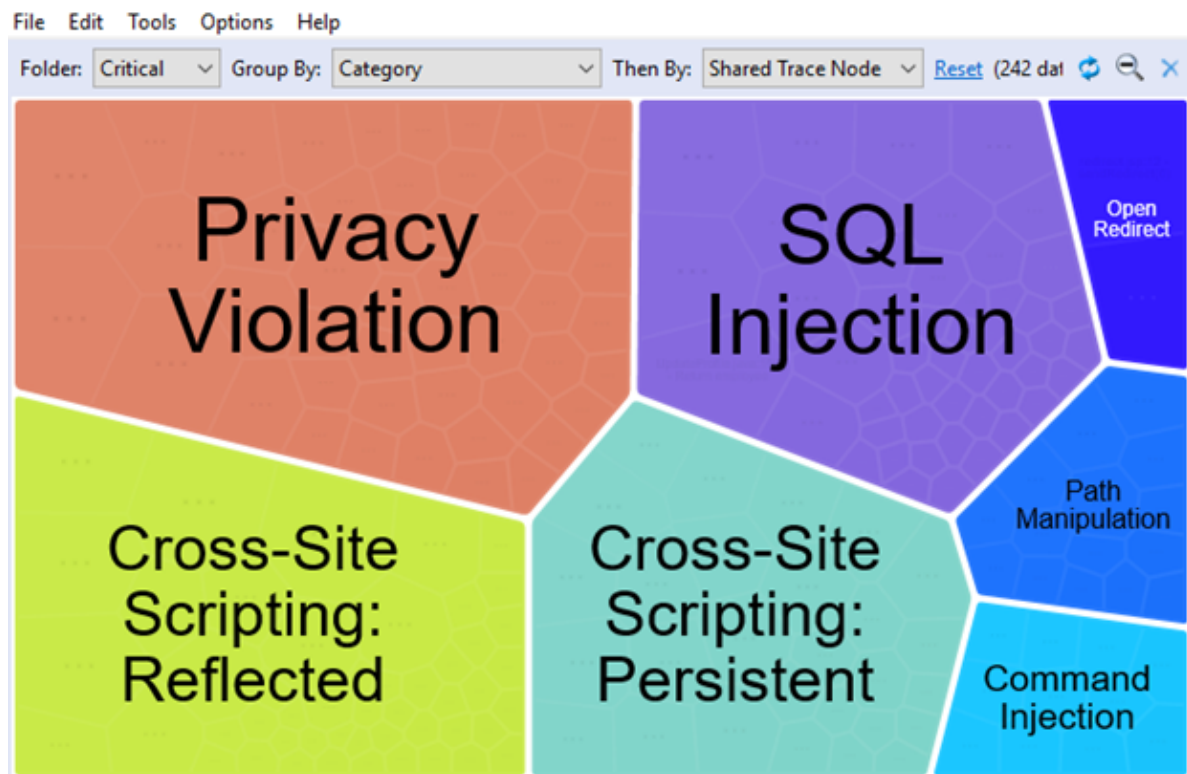
Using Smart View

Smart View provides a visual representation of the dataflow issues in your code so that you can quickly identify optimal remediation or triage strategies for multiple issues at once. To use Smart View:

1. Select **Tools > Smart View**.

Note: Smart View uses the currently selected folder and grouping option.

The number of issues for the currently selected folder and grouping selection determines the relative size of the Smart View tiles.



Note: You can adjust the opacity of the parent tile. For instructions, see "[Customizing the Issues View](#)" on page 59.

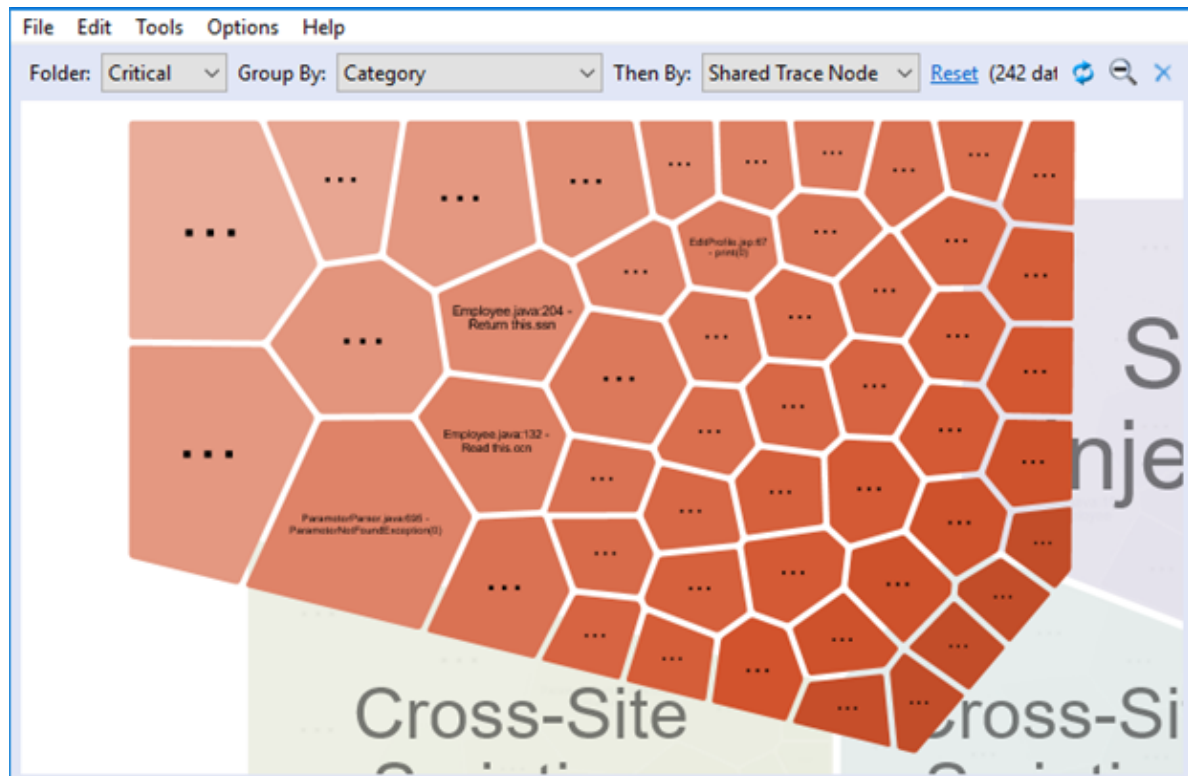
2. To filter the issues that are displayed, you can:


- Select a grouping from the **Folder** list (for example, **Critical**, **High**, **Medium**, **Low**, or **All**)
This list includes any custom folders and folders specific to the current filter set.
- Select a subfolder in the **Group By** list to further sort the issues.
- From the **Then By** list, select whether you are interested in viewing data by **Source**, **Sink**, or **Shared Trace Node**.

Shared Trace Node is a node (or function) in the code that multiple dataflows pass through.


Note: To reset the display to the default Smart View settings, click **Reset**. This resets **Folder** to **Critical**, **Group By** to **Category**, and **Then By** to **Shared Trace Node**.

3. Click a tile to see the issues in each grouping.



Note: To return to the initial grouping level at any time, click **Zoom out** .

4. To see the issues in the auditing interface that share a common dataflow trace node, source, or sink, move your cursor over the tile you are interested in, and then click **View Issues**.
This closes Smart View and returns you to the auditing interface and displays the issues for the selected grouping. The **Group By** category is set to **SmartView** to indicate that you are viewing the results filtered by the Smart View selection. The search box contains the Smart View icon and

the Smart View search criteria:  category:sql injection AND ! [Advanced...](#)

To return to the primary auditing interface at any time, click **Exit Smart View** .

Selectively Displaying Issues Assigned to You

To display only issues assigned to you in the **Issues** view, do one of the following:

- Select the **My Issues** check box.
- Select **Options > Show Only My Issues**.

About Suppressed, Removed, and Hidden Issues

You can control whether the **Issues** view lists the following types of issues:

- *Suppressed* issues—As you assess successive scans of an application version, you might want to completely suppress some exposed issues. It is useful to mark an issue as suppressed if you are sure that the specific vulnerability is not, and will never be, an issue of concern. You might also want to suppress warnings for specific types of issues that are not a high priority or of immediate concern. For example, you can suppress issues that are fixed, or issues that you plan not to fix. Suppressed issues are not included in the group totals shown in the **Issues** view.
- *Removed* issues—As multiple scans are run on a project over time, issues are often remediated or become obsolete. As it merges scan results, Fortify Static Code Analyzer marks issues that were uncovered in a previous scan, but are no longer evident in the most recent Fortify Static Code Analyzer analysis results as Removed. Removed issues are not included in the group totals shown in the **Issues** view.
- *Hidden* issues—You typically hide a group of issues temporarily so that you can focus on other issues. For example, you might hide all issues except those assigned to you. The individuals assigned to address the issues you have hidden in your view can still access them. The group totals displayed in the **Issues** view include hidden issues.

To hide or show suppressed, removed, or hidden issues in the **Issues** view, from the **Options** menu, select (or clear) one or more of the following:

- **Show Suppressed Issues**
- **Show Removed Issues**
- **Show Hidden Issues**

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 **Issues** 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 **Options > 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 **Issues** 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 **Options > 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 **Issues** 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 **Options > 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 <code>java.util.Formatter</code> syntax). See the <code>java.util.Formatter</code> 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.

String	Function
' ... '	Apply the preceding format string to all elements in the selection. This is only valid if the format specification starts with [h] or [v].
%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**.

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 Issues. 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 in `<tools_install_dir>/Core/config/filters/defaulttemplate.xml`
3. Template in `<sca_install_dir>/Core/config/rules/defaulttemplate.xml` or `projecttemplate.xml`
4. Embedded Fortify default template

Configuring Custom Filter Sets and Filters

If the filter sets available in Audit Workbench 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 97](#) and ["Synchronizing Filter Sets and Folders" on page 96](#).

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 **Tools > Project Configuration**.
2. Select the **Filter Sets** tab.

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

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

See Also

["Creating a Filter from the Issues View" below](#)

Creating a Filter from the Issues 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 **Issues** 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.

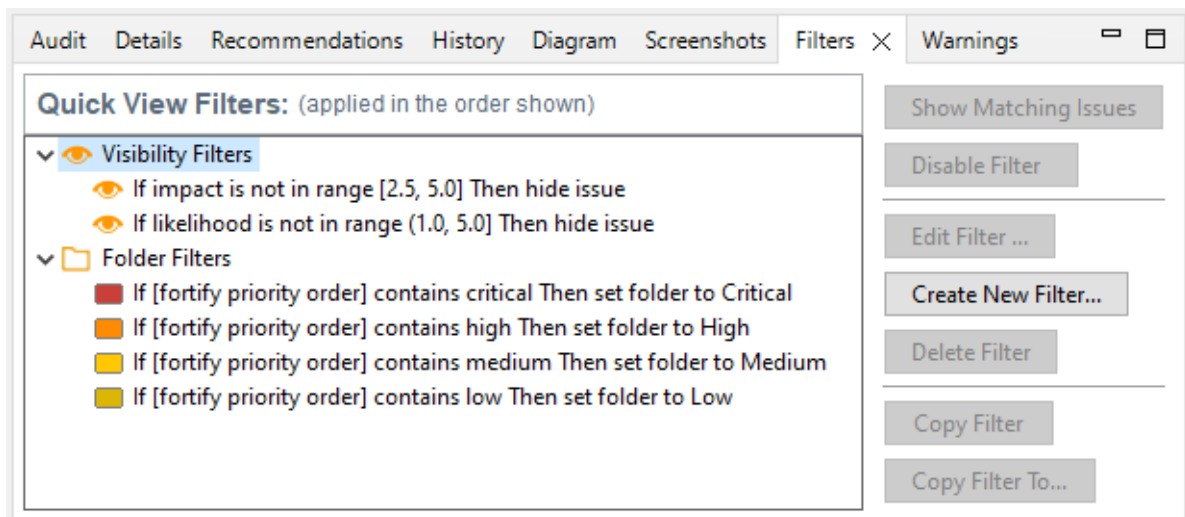
Creating a Filter from the Issue Auditing View

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.

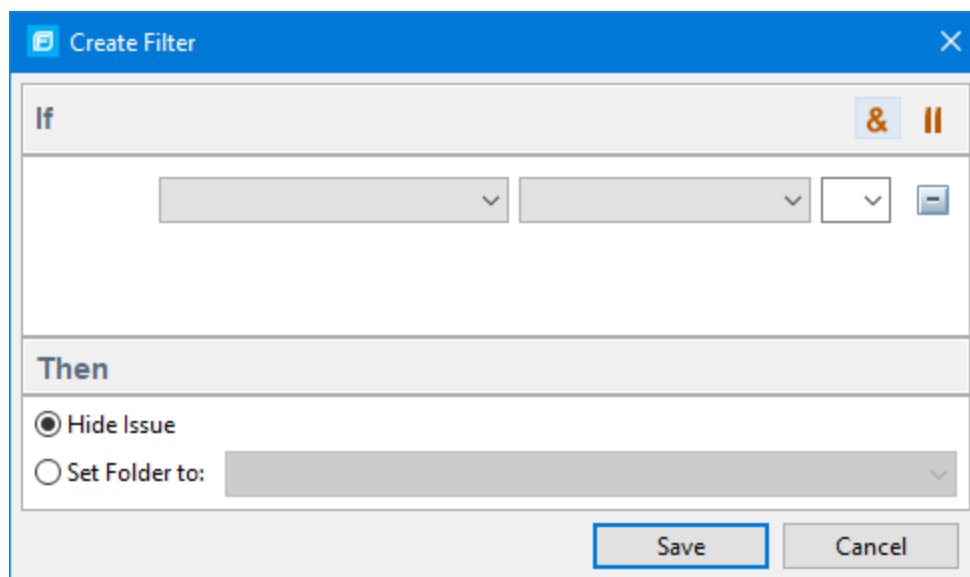
To create a new filter on the **Filters** tab:

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 63](#). 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 **Issues** 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.

Setting the Default Filter Set

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

1. In the **Issues** view, click the **Filter Set** list, and then select **Edit**.

The Project Configuration dialog box opens to the **Filter Sets** tab.

2. In the **Filter Sets** list, select the filter set you want to use as the default for the issue template.
3. Select the **Default filter set** check box, and then click **OK**.

Managing Folders

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

Creating a Folder

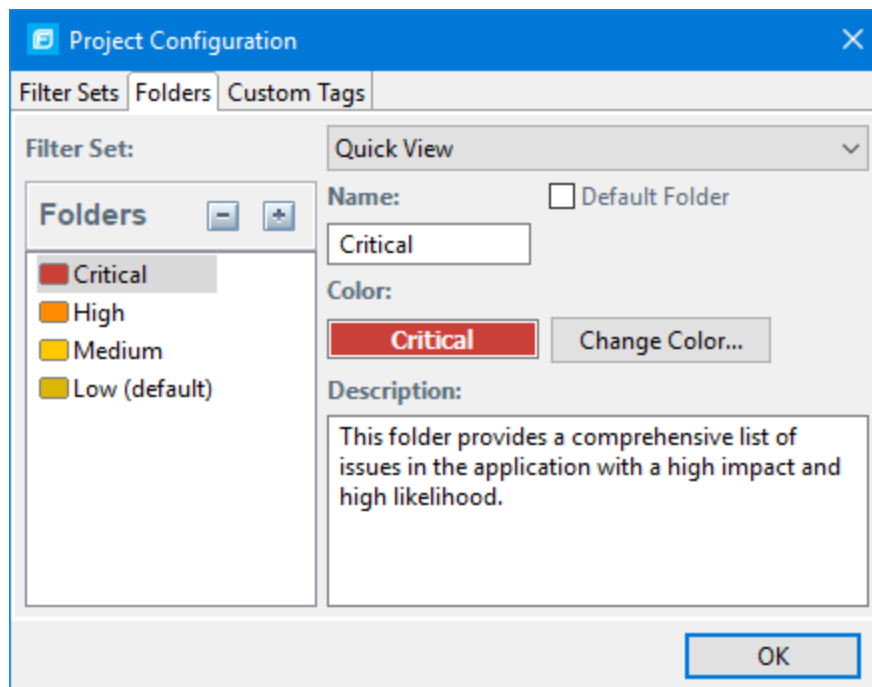
You can create a new folder so that you can display a group of issues you have filtered to the folder. Folders must have unique names.

Note: If this functionality is restricted to administrator users, and you are not an administrator, you cannot create folders.

To create a new folder:

1. Select **Tools > 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 **Add Folder** .

The Add Folder dialog box opens.

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

- b. Type a unique name for the new folder, and then select a folder color.
 - c. Click **OK**.
The folder is added to the bottom of the folder list.
5. In the **Description** box, type a description for the new folder.
 6. To change the tab position of the folder on the **Issues** 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 Issues View" on page 84](#) and ["Creating a Filter from the Issue Auditing View" on page 85](#).

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 **Tools > 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 **Add Folder** .

The Add New Folder to Filter Set dialog box opens.

Note: If the selected filter set already includes all existing folders, the Create Folder dialog box opens and you can create a new folder for the selected filter set.

5. Select the folder to add to the selected filter set, and then click **Select**.
6. Click **OK**.

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

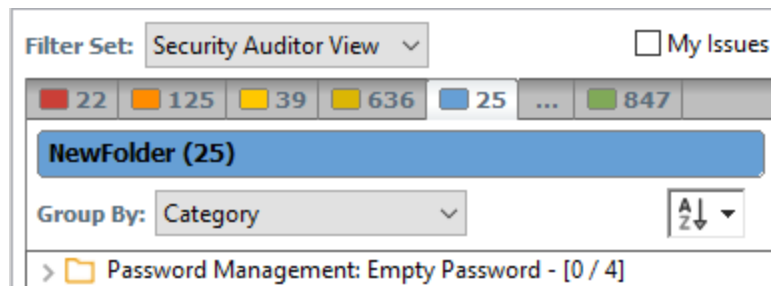
Renaming a Folder

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

To rename a folder:

1. Select **Tools > 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

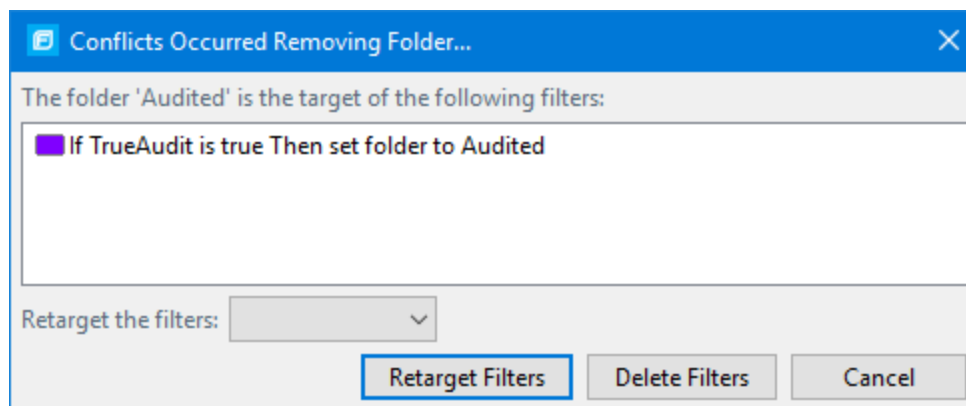
You can remove a folder from a filter set without removing it from other filter sets.

To remove a folder:

1. Select **Tools > 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 **Delete Folder** .

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

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



Do one of the following:

- a. To target the filter to a different folder, select a folder from the **Retarget the filters** list, and then click **Retarget Filters**.
 - b. To delete the filter, click **Delete Filters**, and then click **Yes** to confirm the deletion.
5. Click **OK** to close the Project Configuration dialog box.

The folder is no longer displayed as a tab in the **Issues** 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 also define custom tags from Fortify Software Security Center, either directly with issue template uploads through Fortify Software Security Center, or from Fortify Audit Workbench through issue templates in FPR files.

Note: Although you can add new custom tags from Fortify Audit Workbench as you audit a project, if these custom tags are not defined in Fortify Software Security Center for the issue template associated with the application version, then the new tags are lost if you upload the FPR file to Fortify Software Security Center.

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.
- Hidden (Fortify Software Security Center only)—Use this setting to hide a tag from an application version or issue template.

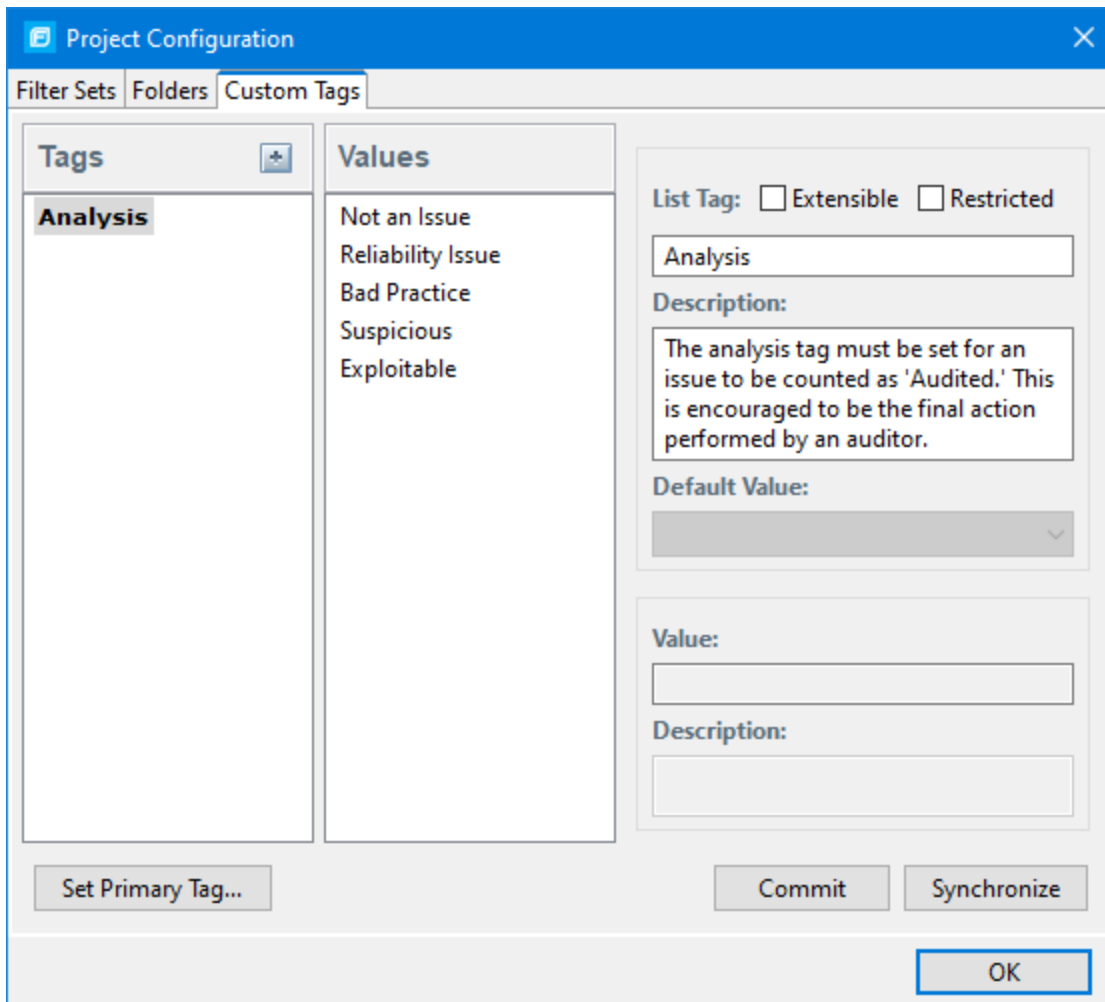
After you define a custom tag, it is displayed below the **Analysis** tag, which enables you to specify values as they relate to specific issues. Custom tags are also available in other areas of the interface, such as in the **Group By** list to group issues in a folder, in the search field as a search 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 **Tools > Project Configuration**.
2. Select the **Custom Tags** tab.



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


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.

Important! Make sure that the name you specify for a custom tag *is not* a database reserved word.

5. From the **Type** list, select one of the following tag types:
 - **List**—Accepts selection from a list of values that you specify for the tag
 - **Date**—Accepts a calendar date

- **Decimal**—Accepts a number with a precision of up to 18 (up to 9 decimal places)
 - **Text**—Accepts a string with up to 500 characters (HTML/XML tags and newlines are not allowed)
6. Click **OK**.
The **Tags** list now includes the new tag.
 7. Configure any or all the following optional tag settings:
 - To allow users to add new values for a list-type tag in an audit, leave the **Extensible** check box selected.
 - To allow only administrators, security leads, and managers to set this tag on an issue, select the **Restricted** check box.
 - Type a description of the custom tag in the **Description** box.
 - For a list-type tag, from the **Default Value** list, select the default value for the tag.
If you do not specify a default value, the default is null.
 8. To add a value for a list-type tag, do the following:
 - a. From the **Tags** list, select the tag name.
 - b. Next to **Values**, click **Add Value** .
 - c. In the Enter Value dialog box, type a value, and then click **OK**.
 - d. Type a description of the value in the **Description** box.
 - e. Repeat steps a through d for each additional value required for the new tag.
 9. To make this custom tag the primary tag:

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

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

The primary tag 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 **Issues** 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 **Tools > 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 **Hide Tag** .

This action hides the tag from your available custom tags. You can make this tag available again when you add a custom tag (see ["Adding a Custom Tag" on page 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 **Tools > 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 22](#).

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 **Tools > 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 22.
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](#)" on the next page. 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 **Tools > 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 **Tools > 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.

Synchronizing Filter Sets and Folders

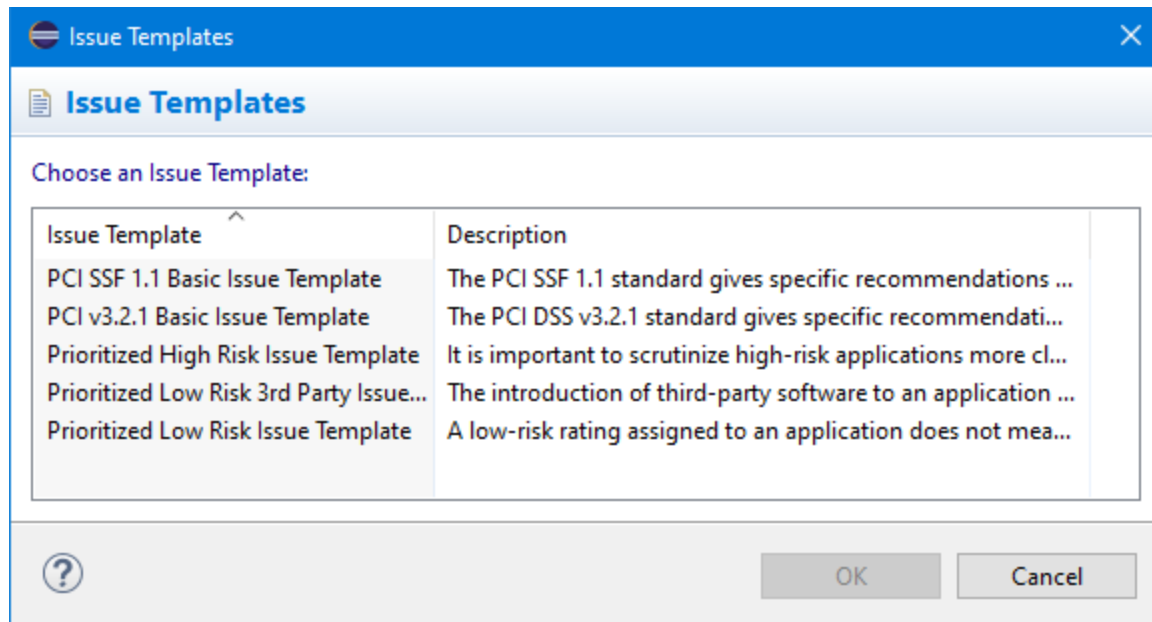
To download filter sets and folders configured from Fortify Software Security Center:

1. Select **Tools > 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 22.](#)



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 Audit Workbench downloads the filter sets and folders from the selected issue template in Fortify Software Security Center, and overwrites your current issue template.

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 **Tools > 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 22.](#)

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**.

Advanced Configuration

This section contains the following topics:

- ["Integrating with a Bug Tracker Application" below](#)
- ["Public APIs" on the next page](#)
- ["Penetration Test Schema" on the next page](#)

Integrating with a Bug Tracker Application

Audit Workbench provides a plugin interface to integrate with bug tracker applications. This enables you to file bugs directly from Audit Workbench. 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 **Tools > Select Bug Tracker**.
3. Select a bug tracker from the list, and then click **OK**.

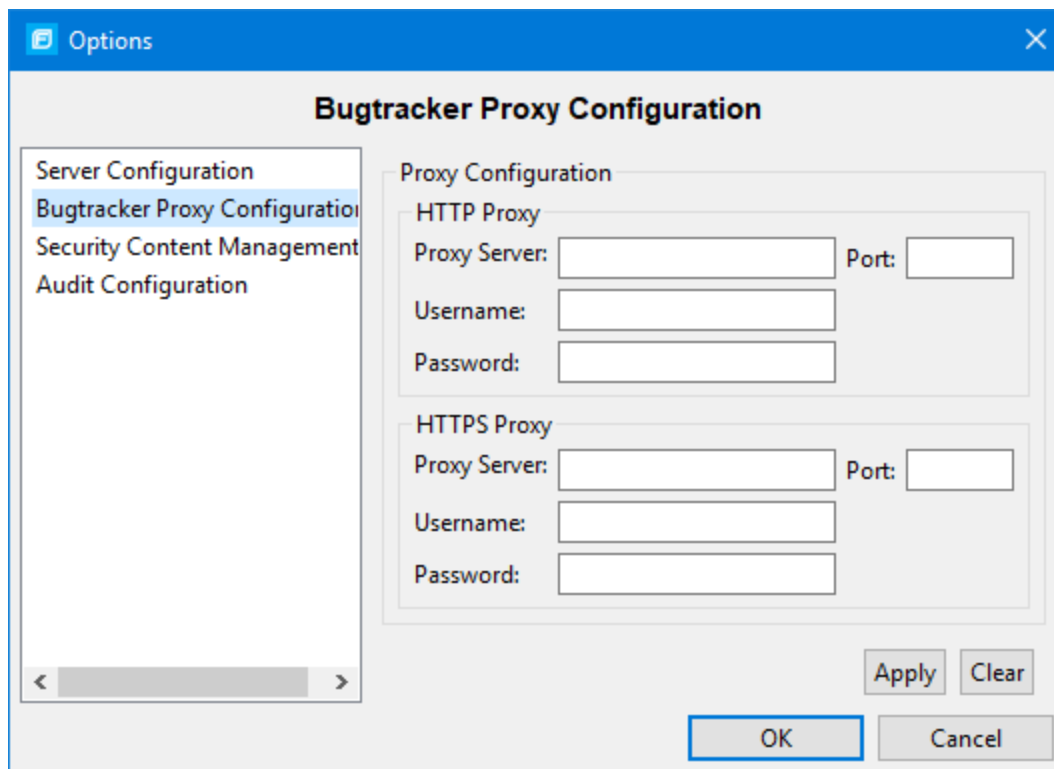
For bug tracker plugin components selected in the Fortify Applications and Tools installation, sample source code is available in `<tools_install_dir>/Samples/bugtrackers/BugTrackerPlugin<bug_tracker_app>`, where `<bug_tracker_app>` is the name of the bug tracker application. To write your own plugin, 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. Fortify Audit Workbench provides the proxy settings to the bug tracker plugin.

To configure proxy settings for bug tracker integration:

1. Select **Options > 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.

Public APIs

Fortify publishes public APIs so that you can create custom parsers for pentest tools and services that are not included in the default distribution. The APIs are in (fortify-public-*.jar), and you can use them to compile your custom parser.

Penetration Test Schema

Fortify also provides a generic penetration test schema (pentestimport.xsd) that you can view in `<tools_install_dir>/Core/config/schemas`. This provides another option for importing additional pentest results. Instead of creating a custom parser for your tool or service, you can translate the results into the Fortify generic format (using XSLT or a similar technology). You can then open or merge these translated results automatically. See ["Penetration Test Results" on page 112](#) for more information.

Chapter 5: Auditing Analysis Results

When Fortify Static Code Analyzer scans application source code, its discoveries are presented as potential vulnerabilities rather than actual vulnerabilities. Every application is unique, and all functionality runs within a context that the development team understands best. No technology can fully determine whether a suspect behavior is considered a vulnerability without direct developer confirmation.

For example, Fortify Static Code Analyzer might discover that a web page designed to display data to the user (for example, a financial transaction record page) appears to allow any authenticated user to request any data with no check of viewing permission. Whether or not this behavior is considered a vulnerability depends entirely on the intended design of the application. If the application is supposed to allow any user to see all data, then the auditor can mark the discovery as a non-issue; otherwise, the auditor can mark the issue as a vulnerability for the team to address.

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 Fortify Audit Workbench.

This section contains the following topics:

- [Working with Audit Projects](#) 100
- [Evaluating Issues](#) 104
- [Submitting an Issue as a Bug](#) 108
- [Correlation Justification](#) 109
- [Penetration Test Results](#) 112

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.

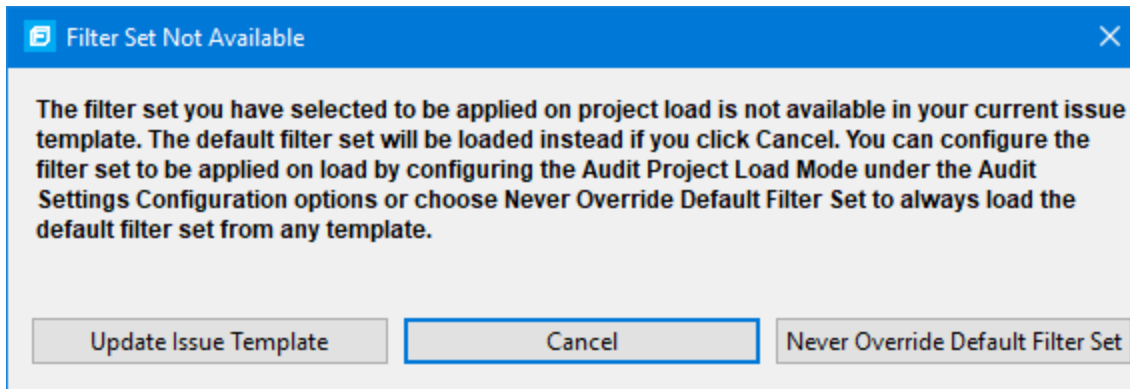
Opening an Audit Project

To open an audit project:

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

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**.

Performing a Collaborative Audit

You can audit a project in Fortify Software Security Center collaboratively with other Fortify Software Security Center users. You can open an application version in Fortify Software Security Center, apply your audit evaluation, and then upload the audit project back to Fortify Software Security Center.

To start a collaborative audit:

1. Start Fortify Audit Workbench.
If you already have an audit project open, close it.
2. Under **Collaborative Applications**, click **Sign In**.
3. Type your Fortify Software Security Center logon credentials.
For information about logging into Fortify Software Security Center, see ["Logging in to Fortify Software Security Center" on page 22](#).
Fortify Audit Workbench displays a list of applications that you have permission to access.

4. Select an application version to audit.

To quickly find an application version, type the name or partial name of an application in the **Search** box. The search is case-insensitive. To clear the search results, clear the **Search** box.

If necessary, click **Refresh** to update the list of applications in Fortify Software Security Center.

The audit project file is downloaded from Fortify Software Security Center and opened in Fortify Audit Workbench.

5. Audit the project as described in ["Evaluating Issues" on page 104](#).
6. When you have completed the audit, select **Tools > Upload Audit Project**.

Note: If necessary, you can refresh your Fortify Software Security Center audit permission settings. See ["Refreshing Permissions from Fortify Software Security Center" below](#).

See Also

["Uploading Audit Results to Fortify Software Security Center" on the next page](#)

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 Audit Workbench.

To refresh your permissions from Fortify Software Security Center:

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

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), Fortify Audit Workbench 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 Fortify Audit Workbench.
2. Select **Tools > 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.

Note: After you select an FPR, Fortify Audit Workbench might prompt you to choose between the issue template in the current FPR and the issue template in the FPR you are merging in.

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.

Merging Audit Data Using the Command-Line Utility

You can also use the FPRUtility command-line utility to merge audit data. This utility enables you to merge an audited project, verify the signature of the FPR, or display analysis results information from an FPR. For more information about how to use this utility, see the *OpenText™ Fortify Static Code Analyzer Applications and Tools Guide*.

Additional Metadata

Each issue in Audit Workbench contains additional metadata that is not produced by the Fortify internal analyzers. Examples include alternative categories (for example, OWASP, CWE, WASC), and prioritization values that are used in the default filters (for example, impact, accuracy, probability). You can view the metadata attributes through the standard grouping and search mechanisms.

If you open an older FPR that does not contain metadata values, the metadata values for the issues are retrieved from legacy mapping files. These legacy mapping files exist in the `<tools_install_dir>/Core/Config/LegacyMappings` directory, and are indexed by either issue category, or issue category and analyzer. The legacy mapping files are accessed as needed, so each issue in your project must always have metadata values, whether those values come from the FPR, the legacy mapping files, or a combination of the two.

Uploading Audit Results to Fortify Software Security Center

When you work on a collaborative audit and you download the audit project from Fortify Software Security Center, Audit Workbench 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 **Options > 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 97 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 **Tools > 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 22.
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 Audit Workbench 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 **Issues** view (see "[About Viewing Analysis Results](#)" on page 39).

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 **Select Date**  to select a date from a calendar.

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

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 **Issues** view, select the issues that you want to assign the same analysis value.
2. Press **Ctrl + Shift + A** (**Cmd + Shift + A** on macOS).

Audit Workbench 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.

Audit Workbench 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 **Options > 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. Audit Workbench 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 **Issues** view, select the issue, and then, on the **Audit** tab in the Issue Auditing view, click **Suppress** .
- In the **Issues** view, right-click the issue, and then click **Suppress Issue**.

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

To display issues that have been suppressed, select **Options > Show Suppressed Issues**.

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

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


- Right-click the issue in the **Issues** 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 integration between the applications has been configured.


To submit an issue as a bug:

1. Select the issue in the **Issues** view, and then, on the **Audit** tab, click **File Bug** .
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 page 98.
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, Fortify Audit Workbench uses the proxy settings specified for bug trackers. For more information, see "[Configuring Proxy Settings for Bug Tracker Integration](#)" on page 98.
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 **Issues** view, and then, on the **Audit** tab, click **File Bug** .
- 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.

Correlation Justification

A correlation occurs when an issue uncovered by one analyzer (Fortify WebInspect Agent, Fortify Static Code Analyzer, or Fortify WebInspect) is related directly or indirectly to an issue uncovered by another analyzer.

Correlated events help you identify issues that have a higher probability of being exploited. A vulnerability that is linked to other vulnerabilities might represent an issue that has multiple points of entry. For example, if Fortify WebInspect scan results are correlated with Fortify Static Code Analyzer scan results, this increases the likelihood that the associated Fortify Static Code Analyzer issues are exploitable.

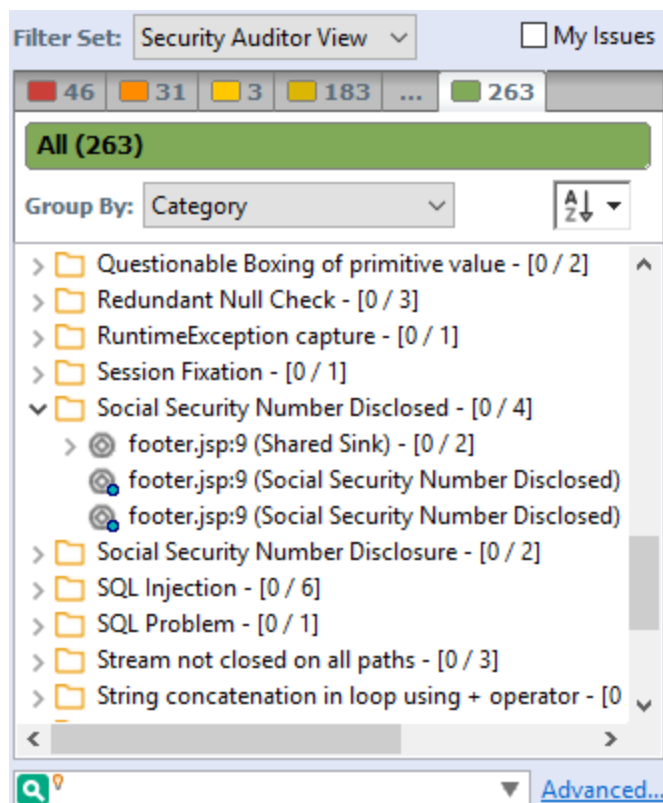
Fortify Audit Workbench provides additional information to help you resolve these correlated issues and mitigate the risks they present. In Fortify Audit Workbench, this additional information is presented as Correlation Justification.

Using Correlation Justification

To use correlation justification:

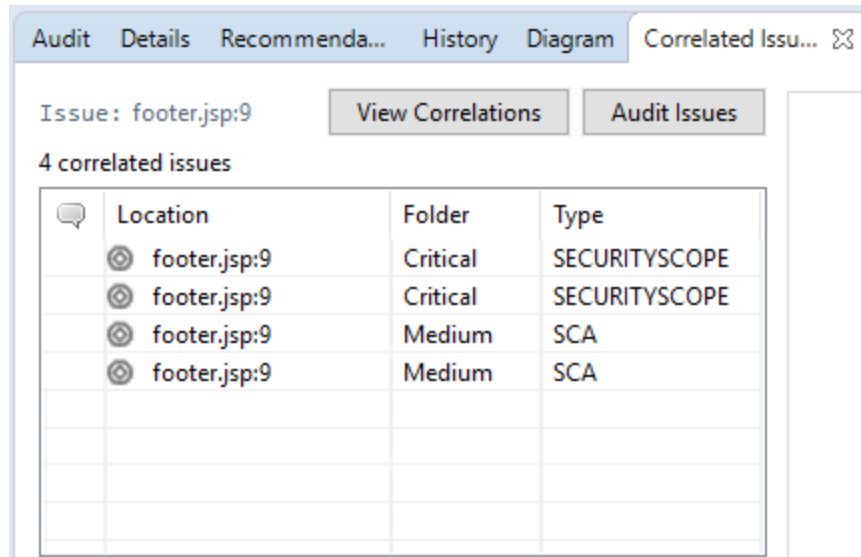
1. In the **Issues** view, select a correlated issue.

A correlated issue is identified in the issues list by a blue sphere on the issue icon, as shown below.



2. In the Issue Auditing view, select the **Correlated Issues** tab.

The **Correlated Issues** tab lists the other issues that are correlated with the issue you first selected.



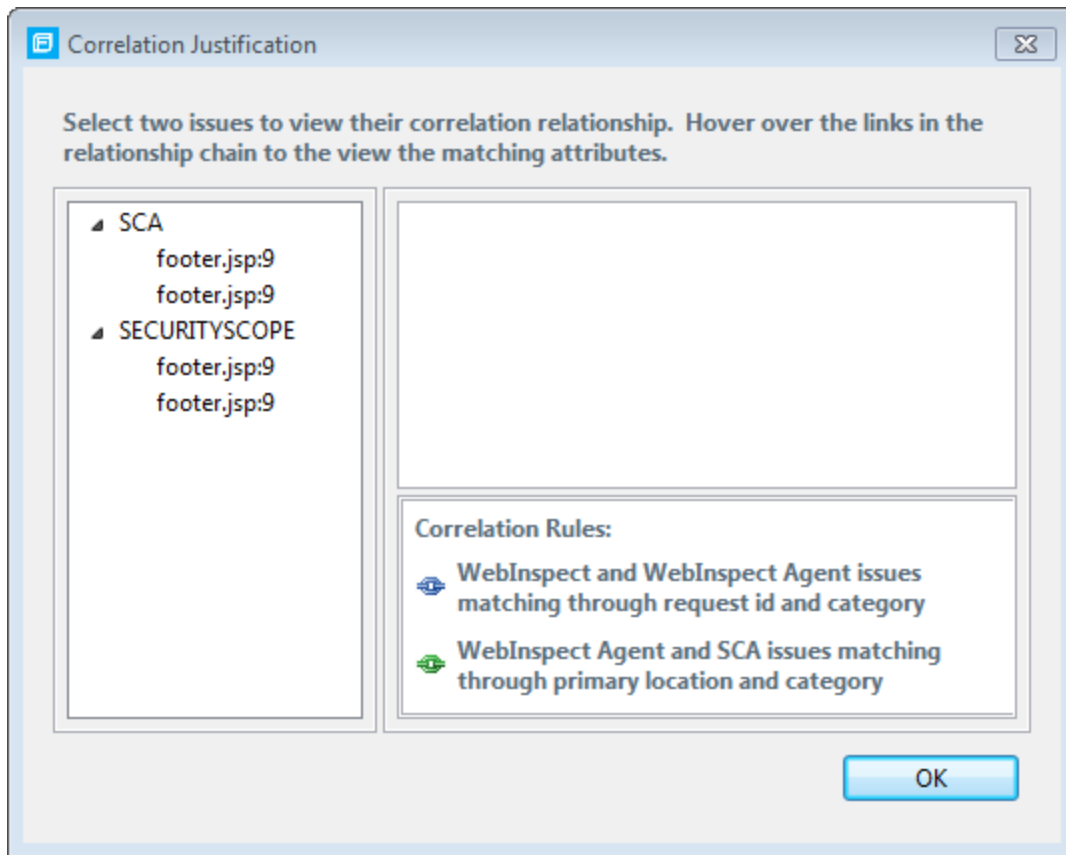
Because you first selected a correlated issue, the **View Correlations** button is available.

3. Click **View Correlations**.

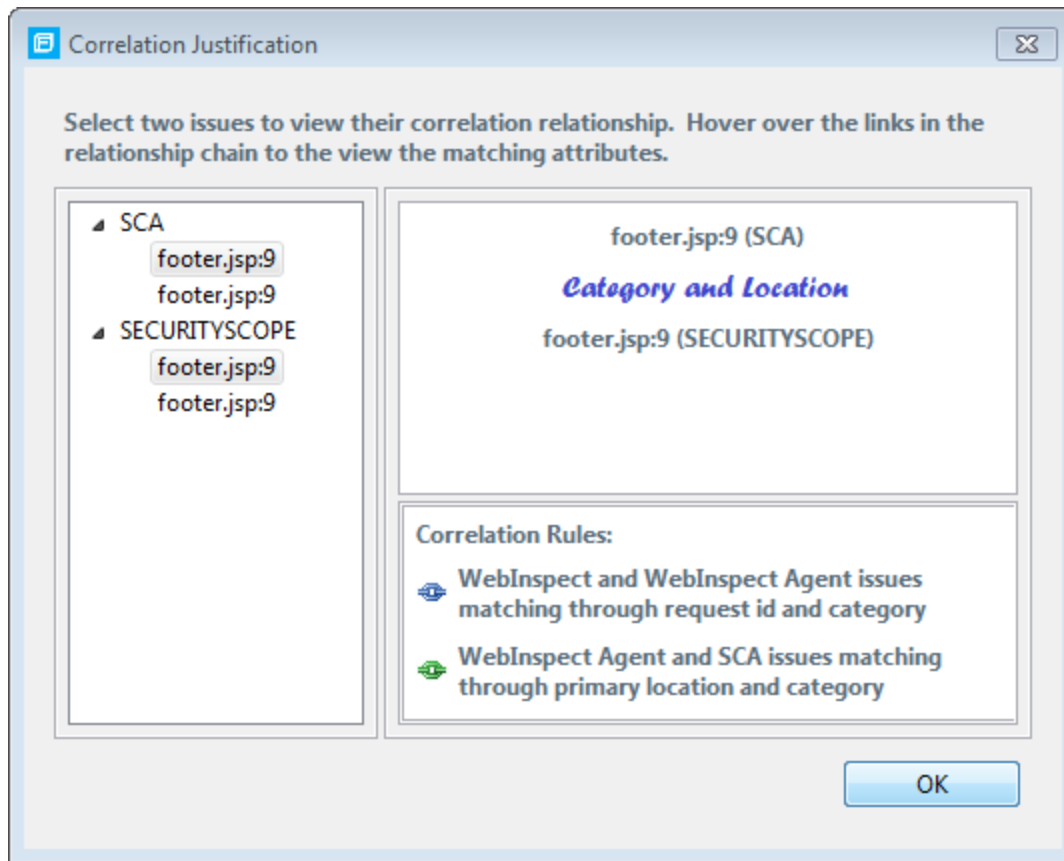
The Correlation Justification dialog box opens and displays the following three panes:

- The correlated issues tree on the left displays all correlated issues within a correlated group, sorted based on analyzers.
- The relationship pane at the top right displays the correlation chain between issues. The chain describes any indirect or direct relationship between the two selected issues.
- The pane at the bottom right describes each correlation rule in the correlation chain displayed

in the relationship pane.



4. To select two issues, press **Ctrl**, and then click each issue.
The relationship pane displays the two issues and their relationships.



5. To inspect the attributes that correlate the issues, move your cursor to each link in the relationship pane.
6. Click **OK**.

Use correlation justification to gain insight into code vulnerabilities and understand why certain issues are correlated. This can help to reduce the time it takes to remediate the issues.

Penetration Test Results

Fortify Audit Workbench supports import of XML for dynamic issues from Fortify WebInspect or from your own custom parser that produces results in an XML file.

To create your own parser, write a class that implements the `com.fortify.pub.issueparsing.AnalysisFileParser` interface from the Fortify public API. It can use any of the classes and utilities from `<tools_install_dir>/Core/lib/fortify-public-<version>.jar`. The Fortify public API documentation is in `<tools_install_dir>/Samples/advanced/JavaDoc/public-api/index.html`. The section for parsing scans and creating issues is in the `com.fortify.pub.issueparsing` package.

Viewing Penetration Test Results

Pentest issues have an `analyzer` attribute equal to `pentest`, and an `analysis_type` attribute that reflects the tool or service (for instance, Fortify WebInspect issues have the `WEBINSPECT` analysis type. You can view these attributes through the standard grouping and search mechanisms.

After you select a pentest issue, Fortify Audit Workbench displays the penetration test details on the **Pentest Details** tab. The following table lists the penetration test details.

Pentest Detail	Description
Request	Click the question mark icon to view the full request.
Path	Web address without the context and parameters.
Referer	Referer header in the request.
Method	Either GET or POST.
Parameters	Parameters included in the HTTP query.
Cookies	Cookies included in the HTTP query.
Attack Type	Type of pentest attack conducted (web address, parameter, header, or cookie).
Attack Payload	Part of the request that causes the vulnerability.
Trigger	Part of the response that shows that a vulnerability occurred. To view the full response, click the question mark icon next to the trigger.

Chapter 6: Generating Analysis Reports

Fortify Audit Workbench provides two types of analysis reports:

- Issue reports based on the Business Intelligence and Reporting Technology (BIRT) system
- Legacy reports based on user-configurable report templates

This section contains the following topics:

[Issue Reports](#) 114

[Legacy Reports and Templates](#) 118

Issue Reports

You can generate issue reports based on the BIRT system from Fortify Audit Workbench or from the command line. For information on how to generate issue reports from the command line using the BIRTReportGenerator utility, see the *OpenText™ Fortify Static Code Analyzer User Guide*.

The following table describes the issue reports available.

Report Template	Description
CWE Top 25	This report lists the most widespread and critical weaknesses that can lead to serious software vulnerabilities (based on the National Vulnerability Database).
CWE/SANS Top 25	This report details issues related to the CWE/SANS Top 25 Most Dangerous Programming Errors and provides information about where and how to fix the issues. It describes the technical risk posed by unremediated issues discovered during analysis and provides an estimate of the development effort needed to test, verify, and fix them.
Developer Workbook	This report provides the information a developer needs to understand and fix the issues discovered during an application audit.
DISA CCI 2	This report provides a standard identifier for policy-based requirements that connect high-level policy expressions and low-level technical implementations.
DISA STIG	This report addresses DISA compliance based on STIG violations and provides information about where and how to fix the issues. It describes

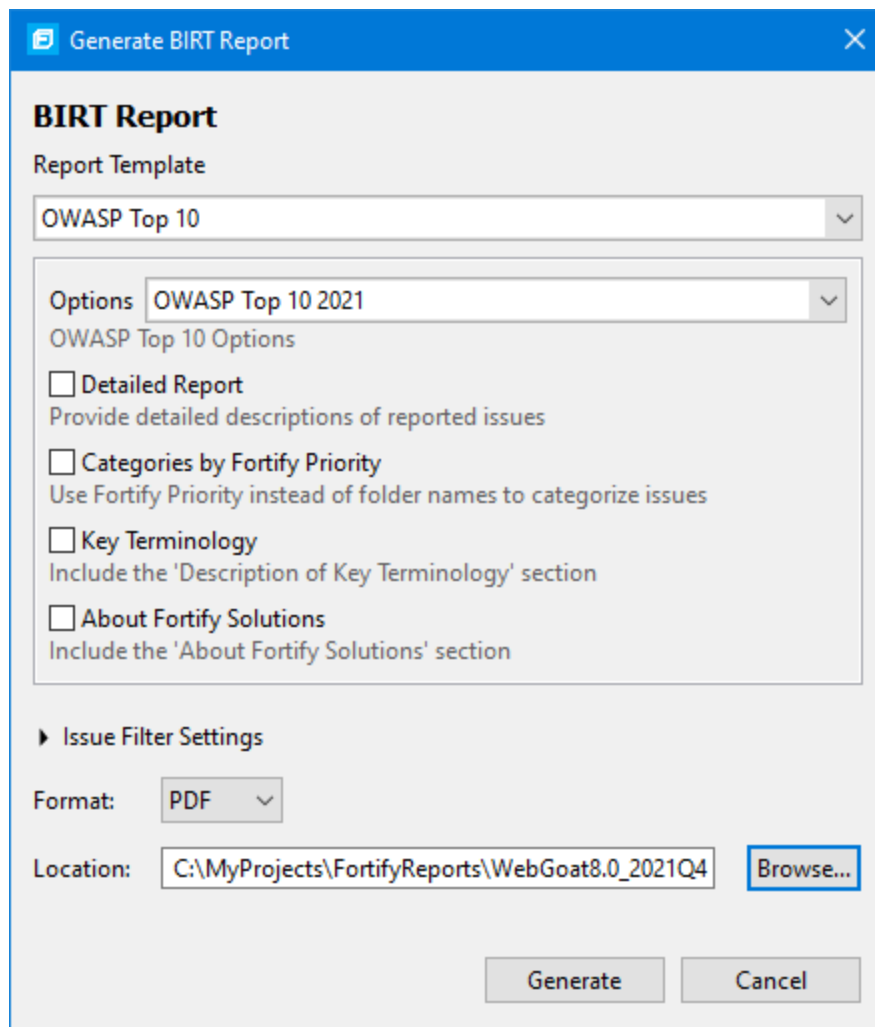
Report Template	Description
	the technical risk posed by unremediated issues and provides an estimate of the development effort required to test, verify, and fix them.
FISMA Compliance: FIPS 200	This report addresses FISMA compliance related to FIPS-200 through controls specified in NIST SP 800-53. It details policy violations and provides information about where and how to fix the issues. It describes the technical risks posed by unremediated violations and provides an estimate of the development effort required to test, verify, and fix them.
GDPR	This report groups all detected issues that are relevant to privacy under the EU General Data Protection Regulation (GDPR) legislation. Use this as a framework to help identify and protect personal data as it relates to application security.
MISRA	This report addresses compliance with either the Motor Industry Software Reliability Association (MISRA) C or C++ guidelines. The results focus on the security relevant guidelines and can help to create a compliance matrix for MISRA. This report describes the technical risk posed by the unremediated issues discovered during analysis and provides an estimate of the development effort needed to test, verify, and fix them.
OWASP API Top 10	This report focuses on weaknesses affecting Web APIs and is intended to be used in combination with other standards and best practices to thoroughly capture all relevant risks. For example, you can use it in combination with the OWASP Top 10 to identify issues related to input validation such as injections.
OWASP ASVS 4.0	This report groups detected issues based on the OWASP Application Security Verification Standard requirements for secure development.
OWASP MASVS 2.0	This report groups detected issues based on the OWASP Mobile Application Security Verification Standard requirements for secure mobile application development.
OWASP Mobile Top 10	This report details the top ten OWASP mobile-related issues and provides information about where and how to fix them. It describes the technical risk posed by the unremediated issues discovered during analysis and gives an estimate of the development effort required to test, verify, and fix them.

Report Template	Description
OWASP Top 10	This report details the top ten OWASP-related issues and provides information about where and how to fix them. It describes the technical risks posed by unremediated issues discovered during analysis and gives an estimate of the development effort required to test, verify, and fix the issues.
PCI DSS Compliance: Application Security Requirements	This report summarizes the application security portions of PCI DSS. It includes tests for 21 application security-related requirements across sections 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is either "In Place" or "Not In Place."
PCI SSF Compliance: Secure Software Requirements	This report summarizes the application security portions of PCI SSF. It includes tests for 23 application security-related control objectives across Control Objective sections 2, 3, 4, 5, 6, 7, 8, and A.2 of PCI SSF and reports whether each control objective is "In Place" or "Not In Place."

Generating Issue Reports

To generate an issue report:

1. Select **Tools > Reports > Generate BIRT Report**.
The Generate BIRT Report dialog box opens.

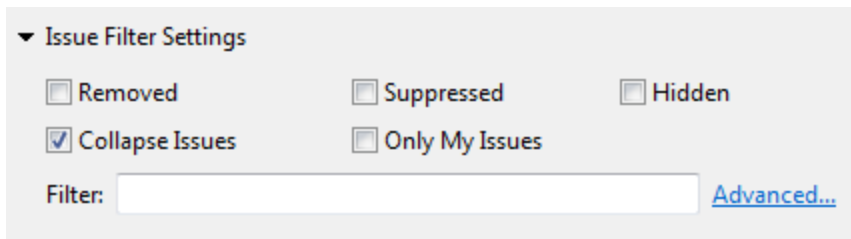


2. From the **Report Template** list, select the type of report you want.
3. From the **Options** list, select the template version (if multiple versions are available).
4. Select the information to include in the report.

Note: Not all options are available for all report templates.

- a. To include detailed descriptions of reported issues, select the **Detailed Report** check box.
- b. To categorize issues by Fortify Priority instead of folder names, select the **Categories By Fortify Priority** check box.
- c. To include descriptions of key terminology in the report, select the **Key Terminology** check box.
- d. To include the About Fortify Solutions section in the report, select the **About Fortify Solutions** check box.

5. To filter information from the report, click **Issue Filter Settings**.



▼ Issue Filter Settings

Removed Suppressed Hidden

Collapse Issues Only My Issues

Filter: [Advanced...](#)

You can filter the issues as follows:

- Click **Removed** to include removed issues in the report.
 - Click **Suppressed** to include suppressed issues in the report.
 - Click **Hidden** to include hidden issues in the report.
 - Click **Collapse Issues** to collapse issues of the same sink and type into a single issue.
 - Click **Only My Issues** to include only issues assigned to your user name.
 - Click **Advanced** to build a search query to further filter the issues to include in the report. For more information about the search modifiers, see ["Search Modifiers" on page 63](#).
6. From the **Format** list, select the format for the report.
You can save the report in the following formats: Portable Document Format (PDF), HTML, and Microsoft Word (DOC).
 7. To specify an alternative location to save the report, click **Browse**, and then select a directory.
 8. Click **Generate**.
 9. If a report with the same file name already exists, you are prompted to either:
 - Click **Overwrite** to overwrite the existing report.
 - Click **Append Version Number** to have the report saved to a file with a sequential number appended to the file name (for example: buildABC CWESANSTop25(1).pdf).

Legacy Reports and Templates

The legacy reports include user-configurable report templates. Report templates provide several optional sections and subsections that gather and present specific types of data. For detailed descriptions of the report templates, see ["Legacy Report Components" on page 145](#). You can generate legacy reports from Fortify Audit Workbench or from the command line using the ReportGenerator utility. For information on how to generate legacy reports from the command line, see the *OpenText™ Fortify Static Code Analyzer User Guide*.

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 **Tools > Reports > 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 Audit Workbench 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 125). 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:

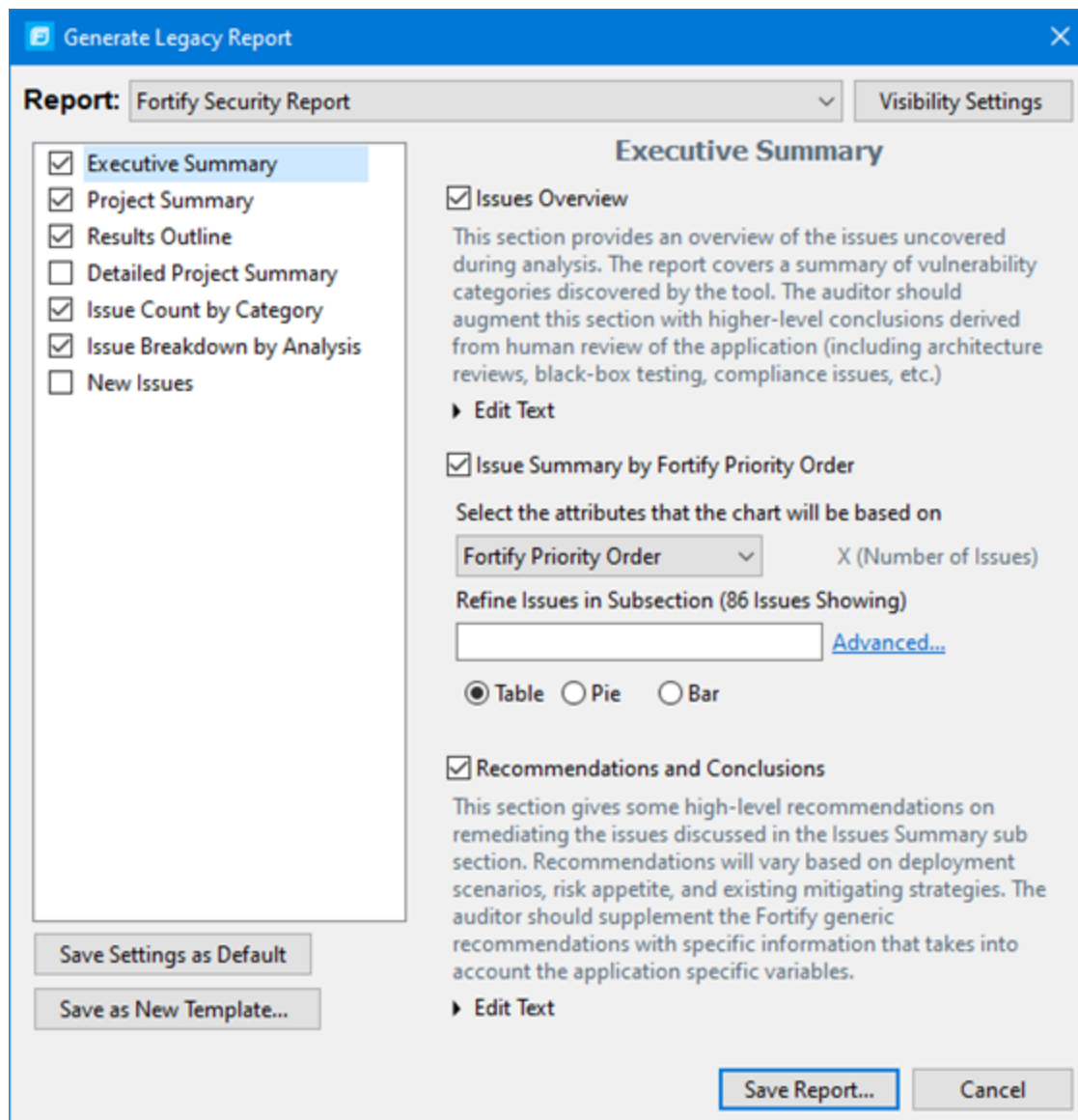
1. Click a section title to view the contents of the section.
The section details are displayed to the right of the dialog box.
2. To include a section in the report, select the section title check box in the list on the left side.
3. To remove a section from the report, clear the check box next to the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

For instructions on how to edit each section, see ["Editing Legacy Report Subsections" on the next page](#).

Opening Legacy Report Templates

To open a report template:

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



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

The Generate 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

Variable	Description
\$PROJECT_NAME\$	Build ID
\$PROPERTIES\$	Complete list of properties set for the analysis phase (same format as project summary)
\$RESULTS_CERTIFICATION\$	Complete certification detail with a list of validity on a per file basis (same format as project summary)
\$RESULTS_CERTIFICATION_SUMMARY\$	Short description of certification (same format as project summary)
\$RULEPACKS\$	Complete list of Rulepacks used for the analysis (same format as project summary)
\$SCAN_COMPUTER_ID\$	Hostname of machine on which the scan was performed
\$SCAN_DATE\$	Date of analysis with the default format style for the locale
\$SCAN_SUMMARY\$	Summary of codebase scanned in format # files, # lines of code
\$SCAN_TIME\$	Time of analysis phase
\$SCAN_USER\$	Username for the user who performed the scan
\$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 73](#).
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 62](#).
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 73](#).
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 62](#).
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 **Tools > 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 **Tools > 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:

```
<tools_install_dir>/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 121](#). 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: Using the Functions View

Fortify Static Code Analyzer identifies all functions declared or called in your source code. You can use the **Functions** view in Fortify Audit Workbench to determine where a function is located in the source code, whether a security rule covered the function, and which rule IDs matched the function. You can also list the functions that Fortify Static Code Analyzer identified as tainted source and view only the functions *not* covered by rules applied in the most recent scan.

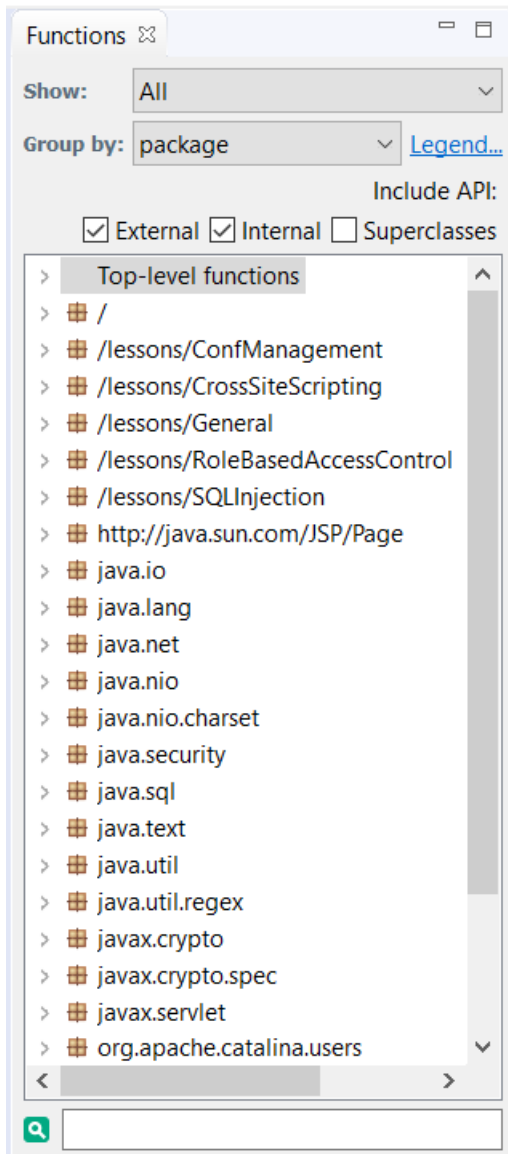
This section contains the following topics:

- [Opening the Functions View](#) 130
- [Sorting and Viewing Functions](#) 131
- [Locating Functions in Source Code](#) 132
- [Synchronizing the Functions View with the Analysis Trace View](#) 132
- [Locating Classes in Source Code](#) 132
- [Determining Which Rules Matched a Function](#) 133
- [Writing Rules for Functions](#) 133
- [Creating Custom Cleanse Rules](#) 134

Opening the Functions View

To open the **Functions** view:

1. Select **Options > Show View > Functions**.



Fortify Audit Workbench displays the **Functions** view in the top-right.

2. To view coverage information about top-level (global) functions, expand the **Top-level functions** node.
3. To view descriptions of the icons displayed to the left of each function, click **Legend**.
 - **Function Not Covered by Rules**
This function does not have any rules associated with it.

Note: It is not necessary to have a rule for every function in an application because not all functions have a security impact.

- **Function Covered by Rules**

This function is covered by one or more rules; however, the rules are never triggered.

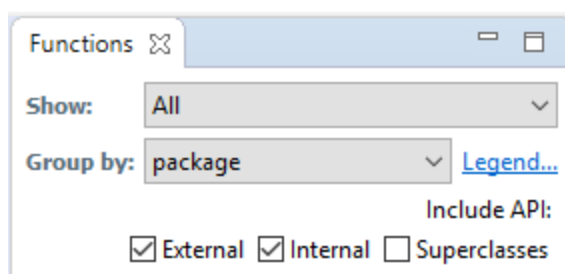
- **Function Covered by Rules and has Matching Rules**

This function is covered by one or more rules and at least one of them triggered. This does not necessarily mean an issue has been found. For example, a tainted data source rule matches the source function but the tainted data that entered the function does not reach a sink.

Sorting and Viewing Functions

To change the order of, or to hide or show functions:

1. Open the **Functions** view.



2. From the **Show** list, select one of the following:
 - To display all functions, select **All**.
 - To display functions not covered by rules, select **Not Covered by Rules**.
 - To display functions that the Rulepack used in the most recent scan has identified as a source of tainted data, select **Taint Sources**.
3. From the **Group By** list, select one of the following sorting methods:
 - To sort functions based on package, select **package**.
 - To sort listed functions by class, select **class**.
 - To sort listed functions alphabetically, select **function**.
4. Under **Include API**:
 - To show functions in external classes, select the **External** check box.
 - To show functions in internal classes, select the **Internal** check box.
 - To show functions in superclasses, select the **Superclasses** check box.

Fortify Audit Workbench updates the **Functions** view.

Locating Functions in Source Code

From the **Functions** view, you can list the file name and line number where the function occurs in the source code.


To show where a function is located in the code:

1. In the **Functions** view, right-click a function, and then select **Find Usages**.
The **Search** view (at center bottom) lists the file locations and line numbers in which the function is used.
2. To jump to a line of code where the function is used, click the corresponding row in the **Search** view.

Synchronizing the Functions View with the Analysis Trace View

You can synchronize the **Functions** view with the **Analysis Trace** view so that, after you select an issue or a trace node from the **Analysis Trace** view, the **Functions** view automatically displays the class that contains the selected item of evidence. This makes it easy for you to inspect other methods in that class, other classes in that package, and so on.


To synchronize the **Functions** view with the **Analysis Trace** view:

1. In the Functions view, from the **Group By** list, select **class**.
2. In the top-right corner of the **Analysis Trace** view, click **Synchronize with Functions View** .
The **Functions** view displays the class that contains the item you selected in the **Analysis Trace** view.

The **Synchronize with Function View** toggles synchronization. To turn off synchronization, click **Synchronize with Functions View** again.

Locating Classes in Source Code

To see where classes are used in the source code:

1. In the **Functions** view, right-click a class , and then select **Find Usages**.
The **Search** view (at center bottom) lists the file locations and line numbers in which the class is used.
2. To jump to a line of code where the class is used, click the corresponding row in the **Search** view.

For functions defined in the source code, you can open the declaration in the **Source** view by right-clicking a function and then selecting **Open Declaration**. The source code is displayed with the line highlighted. Alternatively, you can double-click functions to display the declaration.

Determining Which Rules Matched a Function

You can display the rule ID for all the rules that matched a function. When rules match a function, a green circle icon is displayed next to it.

Fortify Static Code Analyzer can match a rule to functions without finding an issue related to the rule. For example, a tainted data source rule matches the source function but the tainted data entering at that function does not reach a sink.

Note: To use the rule ID to locate related issues, see ["Search Syntax" on page 62](#), or create visibility or folder filters.

To display the rule IDs:

1. Open a project in Fortify Audit Workbench.
2. Open the **Functions** view.
3. Right-click a function, and then select **Show Matched Rules**.

The **Search** view (at center bottom) lists the rule IDs with the vulnerability category name (if applicable) and the Rulepack file name.

Writing Rules for Functions

You can use the Custom Rule Wizard from the **Functions** view to create a rule for a function.

To write a rule for a function:

1. Open a project in Fortify Audit Workbench.
2. Open the **Functions** view.
3. To create a rule:
 - a. Right-click a function, and then select **Generate Rule for Function**.
The Custom Rule Wizard opens.
 - b. Select the rule that best matches the behavior or vulnerability category.
 - c. Provide the information the wizard directs, and save the new rule to a custom Rulepack.
4. To rescan the translated files with the custom Rulepack:
 - a. Select **Options > Options**.
 - b. In the left pane, select **Security Content Management**.
 - c. Click **Import Custom Security Content**.
 - d. Browse to and select the custom Rulepack, and then click **Open**.

- e. Click **OK** to close the Options dialog box.
- f. Click **Scan**.

After the scan is completed, the project is updated.

5. Click **OK**.
6. To verify that the rule matched the function:
 - a. Right-click the function, and then select **Show Matched Rules**.
 - b. Verify that at least one rule ID matches the ID of the rule you created.

The function is now covered by a custom Rulepack and is displayed with a green circle next to it.

Creating Custom Cleanse Rules

You can create custom cleanse rules for specific functions from Fortify Audit Workbench.

To create a cleanse rule for a function:

1. Right-click the function, and then select **Generate Rule for Function**.
The Custom Rule Wizard opens.
2. In the templates list, expand the **DataflowCleanseRule** folder, and then select **Generic Validation Rule**.
3. Click **Next**.
4. On the **Rule Language** step, select the source code language, and then click **Next**.
5. On the **Validation Function Information** step, type the regular expressions for the package, class, and function.
6. Verify that the information is correct, and then click **Next**.
7. Select the argument to cleanse, and then click **Next**.
8. Select the Rulepack to which you want to add the rule, and then click **Finish**.

Chapter 8: Troubleshooting

The following topics provide information on how to troubleshoot problems you might encounter working with Fortify Audit Workbench and how to report an issue to Customer Support.

Creating Archive Logs for Customer Support

You can have Fortify Audit Workbench create an archive file that you can later send to Customer Support to help resolve any support issues that might arise. The file includes your Fortify Audit Workbench logs and system properties.

To create an archive of your Fortify Audit Workbench logs and system properties:

1. In the Fortify Audit Workbench menu bar, select **Help > Contact Fortify Product Support**.
2. In the Create Fortify support archive? dialog box, click **Yes**.
3. Navigate to the folder where you want to save the archive file.
4. Accept the default file name displayed in the **File name** box, or change it.
5. Click **Save**.
6. To contact Customer Support and supply the archive file, follow the instructions in the Save Successful dialog box.
7. Click **OK**.

Using the Debug Option

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

To enable debugging:

1. Navigate to the `<tools_install_dir>/Core/config` directory and open the `fortify.properties` file.
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
<code>com.fortify.Debug</code>	If set to true, all the Fortify Applications and Tools run in debug mode.
<code>com.fortify.awb.Debug</code>	If set to true, Fortify Audit Workbench runs in debug

Property	Description
	mode.
com.fortify.eclipse.Debug	If set to true, the Fortify Plugin for Eclipse runs in debug mode.
com.fortify.VS.Debug	If set to true, the Fortify Extension for Visual Studio runs in debug mode.

Locating Log Files

For help diagnosing a problem, provide log files to Customer Support. To package the log files in a zip, see ["Creating Archive Logs for Customer Support" on the previous page](#).

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 with Fortify Static Code Analyzer.
- C:\Users*username*\AppData\Local\Fortify\AWB-<version>\log
- C:\Users*username*\AppData\Local\Fortify\AWB-<version>\workspace\.metadata\.log

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 with Fortify Static Code Analyzer.
- <userhome>/fortify/AWB-<version>/log
- <userhome>/fortify/AWB-<version>/workspace/.metadata/.log

Addressing the org.eclipse.swt.SWTError Error

On Linux systems, Fortify Audit Workbench can fail to start, resulting in the following error:

```
org.eclipse.swt.SWTError: No more handles [gtk_init_check() failed]
```

If you see this error, check to make sure that X11 is configured correctly and that your DISPLAY variable is set.

Out of Memory Errors

The following two scenarios can trigger out-of-memory errors in Fortify Audit Workbench.

Scenario	More Information
Opening or auditing a large and complex FPR file	"Allocating Additional Memory for Fortify Audit Workbench" below
Running a scan on large and complex project	"Allocating Additional Memory for Fortify Static Code Analyzer" below

As a guideline, assuming no other memory-intensive processes are running, do not allocate more than two thirds of the available system memory.

Allocating Additional Memory for Fortify Audit Workbench

To increase the memory allocated for Fortify Audit Workbench, set the environment variable `AWB_VM_OPTS`. (For example, set `AWB_VM_OPTS=-Xmx4G` to allocate 4 GB to Fortify Audit Workbench.) If you choose to set `AWB_VM_OPTS`, do not allocate more memory than is physically available. Over-allocation degrades performance.

In Fortify Audit Workbench, issue information is persisted to disk. This persisted information is reloaded on demand and thereby decreases the required memory footprint of Fortify Audit Workbench. To prevent out-of-memory errors, you can set a value in the `fortify.properties` file to take advantage of the information persisted to disk functionality. Set the property as follows:

```
com.fortify.model.PersistDataToDisk=true
```

Allocating Additional Memory for Fortify Static Code Analyzer

To increase the memory allocated for Fortify Static Code Analyzer, do one of the following:

- In the Advanced Static Analysis wizard, increase the amount of memory Fortify Static Code Analyzer uses for scanning. This passes the memory allocation option to Fortify Static Code Analyzer. This method does not require restarting Fortify Audit Workbench. See ["Scanning Large and Complex Projects" on page 31](#).
- Before you start Fortify Audit Workbench, set the environment variable `SCA_VM_OPTS`. For example, to allocate 32 GB to Fortify Static Code Analyzer, set the variable to `-Xmx32G`.

Note: If you choose to set `SCA_VM_OPTS`, do not allocate more memory than is physically available. Overallocation degrades performance.

Specifying Memory for External Processes

You can specify how much memory external processes such as iidmigrator use by setting the `com.fortify.model.ExecMemorySetting` property in the `<tools_install_dir>/Core/config/fortify.properties` file. Fortify Audit Workbench uses the iidmigrator tool when merging analysis results. The default memory setting for iidmigrator is 1800 MB. The value for this property setting specifies the maximum heap size.

If you set the value of this property and you have Fortify Static Code Analyzer installed, then in addition to updating the file for Fortify Applications and Tools, make sure to apply the same property change in the `<sca_install_dir>/Core/config/fortify.properties` file.

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, Fortify Audit Workbench 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 Fortify Audit Workbench handles this issue for future occurrences:

1. Select **Options > 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**.

Resetting the Default Views

If you have closed or moved views, such as the **Issues** view or the **Audit** tab, you can reset the user interface to restore the views to the default state.

To reset the user interface to the default state:

1. Select **Options > Options**.
2. In the left pane, click **Audit Configuration**.
3. On the **Appearance** tab, click **Reset Interface**.

Appendix A: Static Analysis Results

Prioritization

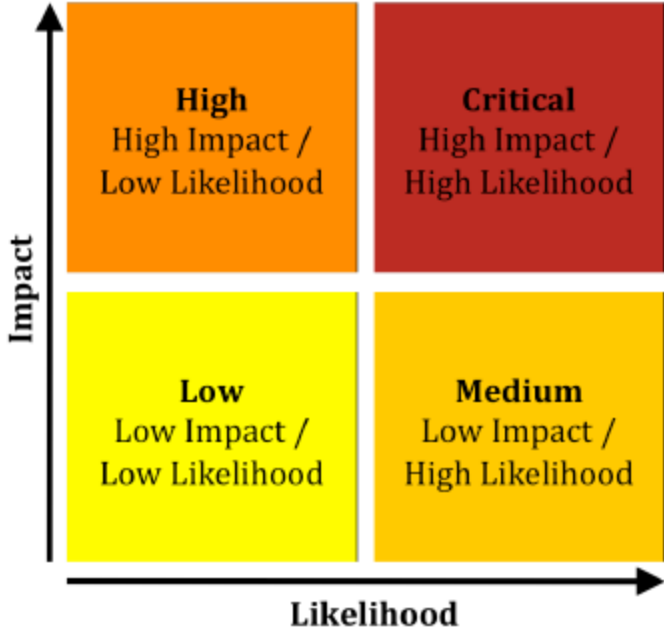
The following topics describe how Fortify Static Code Analyzer automatically prioritizes the scan results displayed in Fortify Audit Workbench.

This section contains the following topics:

- [About Results Prioritization](#)140
- [Quantifying Risk](#)141
- [Estimating Impact and Likelihood with Input from Rules and Analysis](#)142

About Results Prioritization

Fortify Static Code Analyzer divides static analysis findings into four risk quadrants: critical, high, medium, and low. Membership in each quadrant depends on whether the finding has a high or low impact and high or low likelihood of occurring.



When Fortify Static Code Analyzer produces a results file, automated processing and human review can convert issues into findings. Findings, which represent specific problems with the codebase, sometimes map one-to-one with issues. However, in other cases, multiple related issues might be combined into a single finding. For example, every form that submits a request without including a unique token might produce an issue related to Cross-Site Request Forgery (CSRF), but these issues

are more useful when they are combined into a single finding that indicates the application is vulnerable to CSRF attacks.

On occasion, the static analysis process goes wrong. Depending on the rules and the analysis algorithms used, a static analysis can produce false positives (reported vulnerabilities where no vulnerabilities exist) or false negatives (unreported vulnerabilities) or both.

Quantifying Risk

Because it is not possible to determine if or when an organization will suffer consequences related to a vulnerability, Fortify Static Code Analyzer takes a probabilistic approach to prioritizing vulnerabilities. Risk is defined quantitatively, as follows:

$\text{risk} = \text{impact} \times \text{likelihood}$

The risk that a vulnerability poses is equal to the impact of the vulnerability multiplied by the likelihood that the impact will occur. Impact is defined as the negative outcome resulting from a vulnerability and likelihood as the probability that the impact will happen.

Impact can come in many forms. For example, an organization might lose money or reputation because of a successful attack, or it might lose business opportunity because the presence of a vulnerability causes a system to fail a regulatory compliance check.

Two factors contribute to the likelihood that a vulnerability will cause harm:

- The probability that the vulnerability will be discovered (by an attacker or an auditor)
- The conditional probability that, once found, the vulnerability will be exploited

These probabilities change as the computer security field advances. New vulnerability assessment techniques make it easier to find vulnerabilities, and new attack techniques increase the set of vulnerabilities that attackers can exploit. Progressively better vulnerability prevention, mitigation, and recovery strategies help counterbalance these advances.

For example, consider Race Condition: Singleton Member Field vulnerabilities, which occur when code assigns a value associated with a user session to a member variable of a singleton object in a web application. Under the singleton model, the same class instance services all requests, therefore values from one user session can spill over into another user's session. The following code demonstrates a singleton member field race condition:

```
public class GuestBook extends HttpServlet {
    String name, password;
    protected void doPost (HttpServletRequest request,
        HttpServletResponse response) {
        name = request.getParameter("username");
        password = request.getParameter("password");
        if (DBUtils.lookupUser(username, password)) {
            accessSensitiveResources();
        }
    }
}
```

Although this vulnerability is simple to exploit after it is found, it can be difficult to find race conditions because successful attacks often depend on very precise timing. Therefore, this class of vulnerability has a low likelihood of occurring, which primarily reflects the difficulty involved in finding the vulnerability.

For an example of a vulnerability whose likelihood is primarily governed by how difficult it is to exploit, consider HTTP Header Manipulation, which occurs when unvalidated user input is included in an HTTP response header and can enable cross-site scripting, HTTP response splitting, and cache poisoning, among other attacks. The following code demonstrates a header manipulation vulnerability:

```
String author = request.getParameter(AUTHOR_PARAM);
Cookie cookie = new Cookie("author", author);
cookie.setMaxAge(cookieExpiration);
response.addCookie(cookie);
```

In this case, identifying a vulnerable application is often quite simple because the vulnerability is evident in web traffic returned from the server. Crafting a meaningful exploit, however, typically involves a deep understanding of the application's business logic, ready access to a pool of legitimate users, and in some cases, a working knowledge of the network topography between the server and the users. Therefore, this class of vulnerability has a low likelihood because it is difficult to exploit.

Estimating Impact and Likelihood with Input from Rules and Analysis

Fortify Static Code Analyzer estimates the impact of a discovered vulnerability based on its type. The impact value is associated with the static analysis rule that defines the vulnerability. In this way,

results can indicate that a category such as cross-site scripting has a higher impact than a category such as null pointer dereference.

To compute the likelihood portion of the risk equation, Fortify Static Code Analyzer draws on values from the rules used for analysis, the analysis process itself, and from a human auditor (if an individual has reviewed the results.) The likelihood of a finding is computed by combining the accuracy of the rule and the confidence in the analysis with the probability that the vulnerability will be discovered and acted upon, as follows:

$$\text{likelihood} = \text{accuracy} \times \text{confidence} \times \text{probability}$$

For the purpose of weighing static analysis results, an accuracy measure is associated with each rule applied by the analysis engine. This number represents the possibility that the rule will correctly identify a vulnerability.

For example, the rule that Fortify Static Code Analyzer uses to identify the member field race condition has a high accuracy because it precisely identifies assignments to a member field of a singleton object. Conversely, the rule used to identify cross-site request forgery has a low accuracy because it identifies potentially vulnerable form submissions and relies on a human auditor to determine whether the form submissions are susceptible to cross-site request forgery.

During static analysis, Fortify Static Code Analyzer might have to make assumptions about the way the code behaves at runtime. The more assumptions Fortify Static Code Analyzer makes, the more likely it is that a result is incorrect.

The term *confidence* is used to estimate the possibility that Fortify Static Code Analyzer correctly applies the rule. For example, Fortify Static Code Analyzer reports reflected cross-site scripting vulnerabilities in a JSP where data from a request parameter is echoed directly to the page with high confidence. Conversely, Fortify Static Code Analyzer reports a persistent cross-site scripting issue where data read from a database into a class selected at runtime using dependency injection is rendered in the presentation tier with low confidence.

To represent the probability that the vulnerability is discovered and acted upon (with action potentially coming the form of an exploit), Fortify Static Code Analyzer associates a probability measure with each category of vulnerability identified by the rules. For example, cross-site scripting vulnerabilities carry a higher probability than member field race conditions because they are more likely to be discovered and exploited.

From a programmer's perspective, some bugs are harder to fix than others. Modifying a single line of code in a self-contained method is easier than modifying the result of a sequence of calls that span the program. The term *remediation effort* describes the relative amount of effort required to fix and verify a finding.

Fortify Static Code Analyzer provides a remediation effort with each finding it reports. For example, member field race conditions have a small remediation effort, while cross-site request forgery, which often involves major changes to a website, has a high remediation effort.

To avoid implying too much precision where little exists, Fortify Static Code Analyzer limits values of impact, accuracy, confidence, and probability to a decimal range of from 0.1 to 5.0 and scales the calculated likelihood value to the same range. It then defines high values for impact and likelihood as those at 2.5 and above [2.5,5.0] and low values as those below 2.5 (0,2.5).

Fortify Static Code Analyzer does not provide units for remediation effort because the absolute cost of remediating different vulnerabilities differs from one organization to another. Instead, remediation effort estimates the relative cost to remediate one kind of finding versus another, thereby enabling a comparison of the effort required to remediate different vulnerabilities or vulnerabilities across more than one project.

The following table provides sample impact, accuracy, confidence, and probability values for the four vulnerabilities mentioned in this section along with the resulting risk calculations and corresponding remediation effort for each vulnerability category.

Category	Impact	Accuracy	Confidence	Probability	Risk
Race Condition: Singleton Member Field	4	5	5	3	Impact = 4 (High) Likelihood = $(5 \cdot 5 \cdot 3)/25 = 3$ (High) Risk = Critical Estimated remediation effort = 5
Cross-Site Request Forgery	2	1	5	2	Impact = 2 (Low) Likelihood = $(1 \cdot 5 \cdot 2)/25 = <1$ (Low) Risk = Low Estimated remediation effort = 12
Cross-Site Scripting: Reflected	5	5	5	5	Impact = 5 (High) Likelihood = $(5 \cdot 5 \cdot 5)/25 = 5$ (High) Risk = Critical Estimated remediation effort = 1
Cross-Site Scripting: Persistent	5	5	1	5	Impact = 5 (High) Likelihood = $(5 \cdot 1 \cdot 5)/25 = 1$ (Low) Risk = Medium Estimated remediation effort = 1

Appendix B: Legacy Report Components

The following sections provide information about the content and organization of the legacy report templates, which you can either modify or use as provided. Each report template includes several sections and subsections. The subsections provide charting and other data collection and presentation options.

This section contains the following topics:

- Fortify Security Report 145
- Fortify Developer Workbook Report 148
- OWASP Top Ten Reports 149
- Fortify Scan Summary Report 150

Fortify Security Report

The Fortify Security Report is a high-level report that includes comprehensive analysis information and high-level details of the corresponding audit. This report also includes a high-level description and examples of the categories that have the highest priority. The following table lists Fortify Security Report sections and their corresponding subsections.

Section	Subsection
<p>Executive Summary</p> <p>Presents an overview of the scan. This includes an overview of issues, an overview of issues by Fortify Priority Order, and recommendations for issue remediation. This section is designed for management and project managers.</p>	<p>Issues Overview</p> <p>Editable overview of the issues, including the date of the scan, number of issues, name of the project, scan summary, and total number of detected issues.</p>
	<p>Issue Summary by Fortify Priority Order</p> <p>Issues are categorized into the following four risk quadrants based on whether they have a high or low impact, and high or low likelihood of being exploited:</p> <ul style="list-style-type: none"> • Critical - High impact and high likelihood. Critical issues are easy for the attacker to discover and exploit to result in extensive asset damage.

Section	Subsection
	<ul style="list-style-type: none"> • High - High impact but low likelihood. High priority issues are often difficult to discover and exploit, but can result in extensive asset damage. • Medium - Low impact but high likelihood. Medium priority issues are easy to discover and exploit, but often result in little asset damage. • Low - Low impact and low likelihood. Low priority issues are difficult to discover and exploit and typically result in little asset damage. <p>You can present this information in table, pie chart, or bar chart.</p> <p>Recommendations and Conclusions</p> <p>High-level recommendations about how to remediate the issues listed in the Issue Summary by Fortify Priority Order subsection. You can edit the text in this subsection.</p>
<p>Project Summary</p> <p>Provides project summary information such as the codebase, scan information, results certifications, and so on.</p>	<p>Code Base Summary</p> <p>Summary of the analyzed codebase. You can edit the text element of this subsection.</p> <p>Scan Information</p> <p>Analysis details. You can edit the text element of this subsection.</p> <p>Results Certification</p> <p>Results certifications summary. You can edit the text element of this subsection.</p> <p>Attack Surface</p> <p>Attack surface summary. You can edit the text element of this subsection.</p>

Section	Subsection
	<p>Filter Set Summary</p> <p>Summary of the filter set used in the report. You can edit the text element of this subsection.</p> <p>Audit Guide Summary</p> <p>Summary of the audit guide. You can edit the text element of this subsection.</p>
<p>Results Outline</p> <p>Provides an outline of the results that Fortify Static Code Analyzer produced during the scan.</p>	<p>Overall number of results</p> <p>Total number of results that Fortify Static Code Analyzer produced during the scan. You can edit the text element of this subsection.</p> <p>Vulnerability Examples by Category</p> <p>Results summary of highest-level issues by category.</p>
<p>Detailed Project Summary</p> <p>Provides a detailed project summary.</p>	<p>Files Scanned</p> <p>List of all scanned files. You can edit the text element of this subsection.</p> <p>Reference Elements</p> <p>List of all libraries that Fortify Static Code Analyzer used in the translation phase of analysis. You can edit the text element of this subsection.</p> <p>Rulepacks</p> <p>List of Rulepacks that Fortify Static Code Analyzer used in the analysis. You can edit the text element of this subsection.</p> <p>Properties</p> <p>List of properties that Fortify Static Code Analyzer set in the analysis phase. You can edit the text element of this subsection.</p>

Section	Subsection
	<p>Commandline Arguments</p> <p>List of all options that Fortify Static Code Analyzer used in the translation phase of analysis. You can edit the text element of this subsection.</p>
	<p>Warnings</p> <p>List of all warnings issued during both the translation and analysis phases of the scan. You can edit the text element of this subsection.</p>
<p>Issue Count by Category</p> <p>Provides a chart of Issues by category. This chart is configurable.</p>	<p>Issues By Category</p> <p>Chart of issues by category. You can present the information in a table, pie chart, or bar chart.</p>
<p>Issue Breakdown by Analysis</p> <p>Provides a chart of issues by analysis. This chart is configurable.</p>	<p>Issue By Analysis</p> <p>Chart of issues by analysis. You can present the information in a table, pie chart, or bar chart.</p>
<p>New Issues</p> <p>Provides a chart of all new issues. This chart is configurable.</p>	<p>New Issues</p> <p>Chart of new issues. You can present the information in a table, pie chart, or bar chart.</p>

Fortify Developer Workbook Report

The Fortify Developer Workbook report provides a high-level summary of the vulnerabilities detected during a scan. This includes a report summary and an issue summary by Fortify Priority Order. This report is designed for developers. The following table lists Fortify Developer Workbook report sections and their corresponding subsections.

Section	Subsection
<p>Report Overview</p> <p>Provides a high-level overview of report findings.</p>	<p>Report Summary</p> <p>Editable overview of the issues, including the date of the scan, name of the project, scan summary, and total number of detected issues.</p>

Section	Subsection
	<p>Issue Summary by Fortify Priority Order</p> <p>Issues charted based on Fortify Priority Order. You can present the information in a table, pie chart, or bar chart.</p>
<p>Issue Summary</p> <p>Provides the number and categories of vulnerabilities.</p>	<p>Overall number of results</p> <p>Total number of vulnerabilities. You can edit the text element of this subsection.</p>
	<p>Issues by Category</p> <p>Chart of issues based on category. You can present the information in a table, pie chart, or bar chart.</p>
<p>Results Outline</p> <p>Provides an outline of the results that Fortify Static Code Analyzer produced during the scan.</p>	<p>Vulnerability Examples by Category</p> <p>Results summary of highest-level issues by category.</p>

OWASP Top Ten Reports

The OWASP Top Ten reports provide high-level summaries of uncovered vulnerabilities organized based on the top ten issues identified by the Open Web Security Project (OWASP) for years 2004, 2007, 2010, and 2013. These reports include the sections and subsections described in the following table.

Section	Subsection
<p>Report Overview</p> <p>Provides a high-level overview of report findings.</p>	<p>Report Summary</p> <p>Editable overview of vulnerabilities, including the date of the scan, the project name, and the total number of vulnerabilities.</p>
	<p>Issue Summary</p> <p>Chart of issues grouped by a selected attribute such as category, kingdom, or analysis type. You can present the information in a table, pie chart, or bar chart.</p>

Section	Subsection
<p>Issue Breakdown by OWASP Top Ten <year></p> <p>Provides a chart of issues organized by OWASP top ten security risks.</p>	<p>Issue Breakdown by OWASP Top Ten <year></p> <p>Chart of issues grouped by a selected attribute such as category, kingdom, or analysis type. You can present the information in a table, pie chart, or bar chart.</p>
<p>Results Outline</p> <p>Provides an outline of the results that Fortify Static Code Analyzer produced during the scan.</p>	<p>Vulnerabilities by OWASP Top Ten <year></p> <p>List of the vulnerabilities organized by the OWASP Top Ten. You can select the listing to further refine and organize the vulnerabilities that Fortify Audit Workbench provides in the report.</p>

Fortify Scan Summary Report

The Fortify scan summary report type 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. The following table provides descriptions of the report sections and subsections.

Section	Subsection
<p>Issue Count by Category</p> <p>Provides a chart of issues by category.</p>	<p>Issues By Category</p> <p>Chart of issues grouped by a selected attribute such as category, kingdom, or analysis type. You can present the information in a table, pie chart, or bar chart.</p>
<p>Project Summary</p> <p>Provides project summary information, including codebase summary and general scan information.</p>	<p>Code Base Summary</p> <p>Summary of the codebase that Fortify Static Code Analyzer scanned, including the location of the code, the number of files, lines of code, and the build label. You can edit the text element of this subsection.</p>
	<p>Scan Information</p> <p>Scan information, including the Fortify Static Code Analyzer version, machine name, and the name of the user who ran the scan. You can edit the text element of this subsection.</p>

Section	Subsection
	<p>Results Certification</p> <p>Results certifications information, including the results certification summary and the details of the results certification. You can edit the text element of this subsection.</p>
<p>Detailed Project Summary</p> <p>Provides detailed project summary information including the files scanned, reference elements, and so on.</p>	<p>Files Scanned</p> <p>Lists all files that Fortify Static Code Analyzer scanned. You can edit the text element of this subsection.</p>
	<p>Reference Elements</p> <p>List of libraries that Fortify Static Code Analyzer used during the translation phase. You can edit the text element of this subsection.</p>
	<p>Rulepacks</p> <p>List of Rulepacks that Fortify Static Code Analyzer used during the analysis. You can edit the text element of this subsection.</p>
	<p>Properties</p> <p>List of properties that Fortify Static Code Analyzer set during the analysis phase. You can edit the text element of this subsection.</p>
	<p>Commandline Arguments</p> <p>List of all options that Fortify Static Code Analyzer used in the analysis phase. You can edit the text element of this subsection.</p>
	<p>Warnings</p> <p>List of all warnings issued during both the translation and analysis phases of the analysis. You can edit the text element of this subsection.</p>

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 Audit Workbench 24.2.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!