Hewlett Packard
Enterprise

HPE Security Fortify Audit Workbench

Software Version: 17.10

User Guide

Document Release Date: April 2017
Software Release Date: April 2017

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise Development products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The software is restricted to use solely for the purpose of scanning software for security vulnerabilities that is (i) owned by you; (ii) for which you have a valid license to use; or (iii) with the explicit consent of the owner of the software to be scanned, and may not be used for any other purpose.

You shall not install or use the software on any third party or shared (hosted) server without explicit consent from the third party.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

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

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

https://www.protect724.hpe.com/community/fortify/fortify-product-documentation

You will receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Contents

Preface

Contacting HPE Security Fortify Support

If you have questions or comments about using this product, contact HPE Security Fortify Technical Support using one of the following options.

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

https://support.fortify.com

To Email Support

fortifytechsupport@hpe.com

To Call Support

1.844.260.7219

For More Information

For more information about HPE Security software products: http://www.hpe.com/software/fortify

About the Documentation Set

The HPE Security Fortify Software documentation set contains installation, user, and deployment guides for all HPE Security 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 HPE Security user community website:

https://www.protect724.hpe.com/community/fortify/fortify-product-documentation

You will need to register for an account.

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
17.10	Added: • "Logging in to Fortify Software Security Center" on page 22 - Added information about connecting to HPE Security Fortify Software Security Center with single sign-on credentials. • "Specifying the Default Issue Grouping" on page 37 - New option to specify a default Group By setting Updated: • "Details Tab" on page 46 - Now includes Remediation Effort
16.20	Updated: • "Updating Security Content" on page 21 - New way to view external mappings • "Configuring Custom Tags for Auditing" on page 73 and "Evaluating Issues" on page 85 - New types of custom tags • "Summary Tab" on page 45 and "Evaluating Issues" on page 85 - New Audit Assistant tags
16.10	Added: • "Warnings Tab" on page 49 - Updated analysis warnings view moved from Project Summary to the Issue Auditing view • "Refreshing Permissions From Fortify Software Security Center" on page 83 Updated: • "Scanning Large and Complex Projects" on page 25 and "Scanning Visual Studio Solutions and Projects" on page 30 - Updated interface for selecting Rulepacks • "Adding a Custom Tag" on page 74 - New option to make custom tags restricted • "Uploading Audit Results to Fortify Software Security Center" on page 84 - New instructions for refreshing Fortify Software Security Center permissions • "Generating BIRT Reports" on page 95 - New ability to save in XLS format • Terminology updated to match Fortify Software Security Center

Software Release / Document Version	Change
	Removed: Hotspot filter

Chapter 1: Introduction

This section contains the following topics:

About HPE Security Fortify Audit Workbench

Audit Workbench complements HPE Security Fortify Static Code Analyzer (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 Audit Workbench, you can view and audit FPR files from HPE Security Fortify Software Security Center, HPE Security Fortify Runtime Application Protection, and HPE Security Fortify scanning plugins for IDEs. Audit Workbench issue templates help you sort the results of large scans in a way that works for your business and workflows.

Audit Projects and Issue Templates

After you initiate a source code scan from Audit Workbench, Fortify Static Code Analyzer scans and analyzes the code to produce comprehensive results. Audit Workbench organizes these results into 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 Workbench 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 Audit Workbench (and Fortify Software Security Center) configures and prioritizes the vulnerabilities (issues) uncovered in source code. 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 Audit Workbench.

Hybrid 2.0 Technology

The 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 defects in the source code.

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 Fortify Static Code Analyzer scans uncover. If you connect Audit Workbench to your Fortify Software Security Center instance, 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 and download FPR files
- Perform collaborative audits
- Manage the security content, which consists of HPE Security 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 Audit Workbench)
- Download issue templates
- Upload new and modified issue templates

Related Documents

This topic describes documents that provide information about HPE Security Fortify Audit Workbench.

Note: The Protect724 site location is https://www.protect724.hpe.com/community/fortify/fortify-product-documentation.

All Products

The following documents provide general information for all products.

Document / File Name	Description	Location
HPE Security Fortify Software System Requirements HPE_Sys_Reqs_<*version*>.pdf	This document provides the details about the environments and products supported for this version of HPE Security Fortify Software.	Included with product download and on the Protect724 site
HPE Security Fortify Software Release Notes HPE_FortifySW_RN_<*version*>.txt	This document provides an overview of the changes made to HPE Security Fortify Software for this release and important information not included elsewhere in the	Included on the Protect724 site

Document / File Name	Description	Location
	product documentation.	
What's New in HPE Security Fortify Software <version> HPE_Whats_New_ <*version*>.pdf	This document describes the new features in HPE Security Fortify Software products.	Included on the Protect724 site
HPE Security Fortify Open Source and Third-Party License Agreements HPE_OpenSrc_<*version*>.pdf	This document provides open source and third-party software license agreements for software components used in HPE Security Fortify Software.	Included with product download and on the Protect724 site
HPE Security Fortify Glossary HPE_Glossary.pdf	This document provides definitions for HPE Security Fortify Software terms.	Included with product download and on the Protect724 site

HPE Security Fortify Software Security Center

The following documents provide information about HPE Security Fortify Software Security Center.

Document / File Name	Description	Location
HPE Security Fortify Software Security Center User Guide HPE_SSC_Guide_ <version>.pdf HPE_SSC_Help_<version>	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. 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.	Included with product download and on the Protect724 site
HP Fortify Software Security Center User Guide: Legacy User Interface	This document is the user guide for HP Software Security Center version 4.30. The legacy (4.30)	Included with product download and on the Protect724 site

Document / File Name	Description	Location
HP_Fortify_SSC_User_Guide_Legacy.pdf PDF only; no help file	user interface is available from the Fortify Software Security Center version 16.20 user interface. Specific areas of functionality are available only in the 4.30 interface.	
HPE Security Fortify Software Security Center Process Designer Guide: Legacy User Interface HPE_SSC_Proc_Design_Guide_Legacy_*<version>*.pdf HPE_SSC_Proc_Design_Help_*<version>*	This document provides information about how to start the Process Designer, configure its connection to your Fortify Software Security Center instance, and then use it to work with Fortify Software Security Center process templates, which are used only in the Fortify Software Security Center legacy (version 4.30) user interface.	Included with product download and on the Protect724 site
HP Fortify Software Security Center Installation and Configuration Guide: Legacy User Interface HP_Fortify_SSC_Install_and_Config_Guide_Legacy.pdf PDF only; no help file	This document provides system and database administrators with complete instructions on how to configure Fortify Software Security Center server software using the legacy (v4.30) user interface.	Included with product download and on the Protect724 site
HPE Security Fortify Software Security Center Process Designer Guide: Legacy User Interface HPE_SSC_Proc_Design_Guide_Legacy_*<version>*.pdf HPE_SSC_Proc_Design_Help_*<version>*	This legacy document provides information about how to start the Process Designer, configure its connection to your Fortify Software Security Center instance, and then use it to work with Fortify Software Security Center process templates.	Included with product download and on the Protect724 site

HPE Security Fortify Static Code Analyzer

The following documents provide information about Static Code Analyzer.

Document / File Name	Description	Location
HPE Security Fortify Static Code Analyzer User Guide HPE_SCA_Guide_<*version*>.pdf HPE_SCA_Help_<*version*>	This document describes how to 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.	Included with product download and on the Protect724 site
HPE Security Fortify Static Code Analyzer Installation Guide HPE_SCA_Install_<*version*>.pdf HPE_SCA_Install_Help_<*version*>	This document contains installation instructions for Fortify Static Code Analyzer and Applications.	Included with product download and on the Protect724 site
HPE Security Fortify Static Code Analyzer Performance Guide HPE_SCA_Perf_Guide_<*version*>.pdf PDF only; no help file	This document provides guidelines for selecting hardware to scan different types of codebases and offers tips for optimizing memory usage and performance.	Included with product download and on the Protect724 site
HPE Security Fortify Static Code Analyzer Custom Rules Guide HPE_SCA_Cust_Rules_Guide_<*version*>.zip PDF only; no help file	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.	Included with product download

Chapter 2: Getting Started

The following topics provide an overview of HPE Security 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, Audit Workbench, and any plugins or packages you have installed) as new versions of the products become available.

This section contains the following topics:

About Upgrades

You can check on the availability of new Fortify SCA and Applications (including Audit Workbench) versions from the Audit Workbench user interface. If a version newer than the one you have installed is available, you can download it and upgrade your instance.

You can also configure Audit Workbench to check for, download, and install new versions automatically at startup. Whether you upgrade your Fortify SCA and Applications manually or automatically, your data is preserved.

To enable upgrades from Audit Workbench, a Fortify Software Security Center administrator must first set up the auto upgrade capability on the server host. The following topics address how to set up auto upgrades (as a Fortify Software Security Center administrator) for Audit Workbench and how to perform the upgrades from Audit Workbench.

Enabling Fortify SCA and Applications Updates from Audit Workbench

To make a new Fortify SCA and Applications installer available to Audit Workbench users for upgrades:

1. On the Fortify Software Security Center host, navigate to the `<appserver_deployment_location>/ssc/WEB-INF/internal` directory and open the `securityContext.xml` file in a text editor.
2. Locate the following line:

```
<!-- <security:intercept-url pattern="/update-site/**" access="PERM_
ANONYMOUS"/> -->
```

3. Remove the comment tags from the line of text so that it looks like the following:

```
<security:intercept-url pattern="/update-site/**" access="PERM_
ANONYMOUS"/>
```

4. Save and close the `securityContext.xml` file.
5. Navigate to the <*appserver_deployment_location*>`/ssc/update-site/installers` directory.
6. Open and read the `readme.txt` file.
7. From the `readme.txt` file, copy the sample `update.xml` file content (between and including the `<installerInformation>` and `</installerInformation>` tags, and then paste it into a new text file with the file name `update.xml`.
8. Name the new file `update.xml` and save it to the <*appserver_deployment_location*>`/ssc/update-site/installers` directory.
9. Any time a new Fortify SCA and Applications installer file (`HPE_Security_Fortify_SCA_and_Apps_`<*version*>`_`<*OS*>`.exe`) becomes available, place it in the <*appserver_deployment_location*>`/ssc/update-site/installers` directory.
10. Open the `update.xml` file in a text editor, and then do the following:
    a. In the `versionId` element, type the version ID for the new installer.
       The version ID is the version number without the periods.
       Make sure that the value you type matches the Fortify SCA and Applications version in the installer.
    b. In the `<version>` element, type the version number for the new installer.
11. Save and close your edited `update.xml` file.

Upgrading Manually

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

To check for, and (potentially) install, a newer Fortify SCA and Applications version, do one of the following:

- Select **Help > Check for Upgrades**.

Alternatively,

1. Select **Options > Options**.
   The Options dialog box opens to the **Server Configuration** settings.
2. Under **Audit Workbench Upgrade Configuration** on the right, do the following:
   a. In the **Server URL** box, type the URL for your Fortify Software Security Center server.
   b. Click **Check Now**.

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

Important: If you have an HPE Security Fortify Plugin for Eclipse installed, after you upgrade your Fortify SCA and Applications from Audit Workbench, you must uninstall, and then reinstall the Eclipse Plugin.

Configuring Automatic Upgrades

To configure upgrade checks at Audit Workbench startup:

1. From Audit Workbench, select **Options > Options**.
2. In the left pane, leave **Server Configuration** selected.
3. Under **Audit Workbench Upgrade Configuration** on the right, do the following:
   a. In the **Server URL** box, type the URL for the `installers` folder on your Fortify Software Security Center server.
   b. Select the **Check for upgrades at startup** check box.
4. Click **OK**.

After this, each time you start Audit Workbench, it checks the server to determine whether a newer Fortify SCA and Applications version is available and then, if a newer version is available, downloads and installs it.

Important: If you have an HPE Security Fortify Plugin for Eclipse installed, after you upgrade your Fortify SCA and Applications from Audit Workbench, you must uninstall, and then reinstall the Eclipse Plugin.

Renewing Expired Licenses

The license for Fortify Static Code Analyzer and its tools, including Audit Workbench, expires annually. You can get an updated license from the Fortify Customer Portal.

To update an expired license:

1. Log on to the Fortify Customer Portal (https://support.fortify.com).

   If you do not have an account, contact HPE Security Fortify Technical Support (fortifytechsupport@hpe.com).

   If you encounter a problem logging into your account, send an email to HPE Security Fortify Technical Support (fortifytechsupport@hpe.com) with "Portal Access" as the subject.
2. After you log onto the Fortify Customer Portal, at the top of the page, click the **My Licenses** tab.

   The Download Licenses page lists all licenses with current maintenance agreements. If you do not see your license, email HPE Security Fortify Technical Support (fortifytechsupport@hpe.com) with "Maintenance Renewal Verification" as the subject. If your maintenance agreement was recently renewed, the Download Licenses page might not yet reflect this.

3. Click the link for the license you want to use.
   The license is downloaded automatically to your machine.
4. Start Audit Workbench, and check to make sure that you can log on.

About Starting Audit Workbench

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

Starting Audit Workbench on Windows Systems

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

- Select **Start > All Programs > HPE Security Fortify SCA and Applications <*version*> > Audit Workbench**

where <*version*> is the version you have installed.

Alternatively,

1. Open a Command window, and then change to the `<sca_install_dir>\bin` directory.
2. At the prompt, type `auditworkbench.cmd`.

Starting Audit Workbench on Non-Windows Systems

To start Audit Workbench on a non-Windows system:

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

About HPE Security Fortify Software Security Content

Audit Workbench uses a knowledgebase of rules to enforce secure coding standards applicable to the codebase for static analysis. HPE Security Fortify Software Security Content (security content) consists of Secure Coding Rulepacks and external metadata:

- Secure Coding Rulepacks describe general secure coding idioms for popular languages and public APIs.
- External metadata include mappings from the HPE Security categories to alternative categories (such as CWE, OWASP Top 10, and PCI DSS). You can modify the existing mapping in the external metadata document (`externalmetadata.xml`) or create your own files to map HPE Security issues to different taxonomies, such as internal application security standards or additional compliance obligations (recommended). For instructions on how to create your own custom external metadata, see the *HPE Security Fortify Static Code Analyzer Custom Rules Guide*.

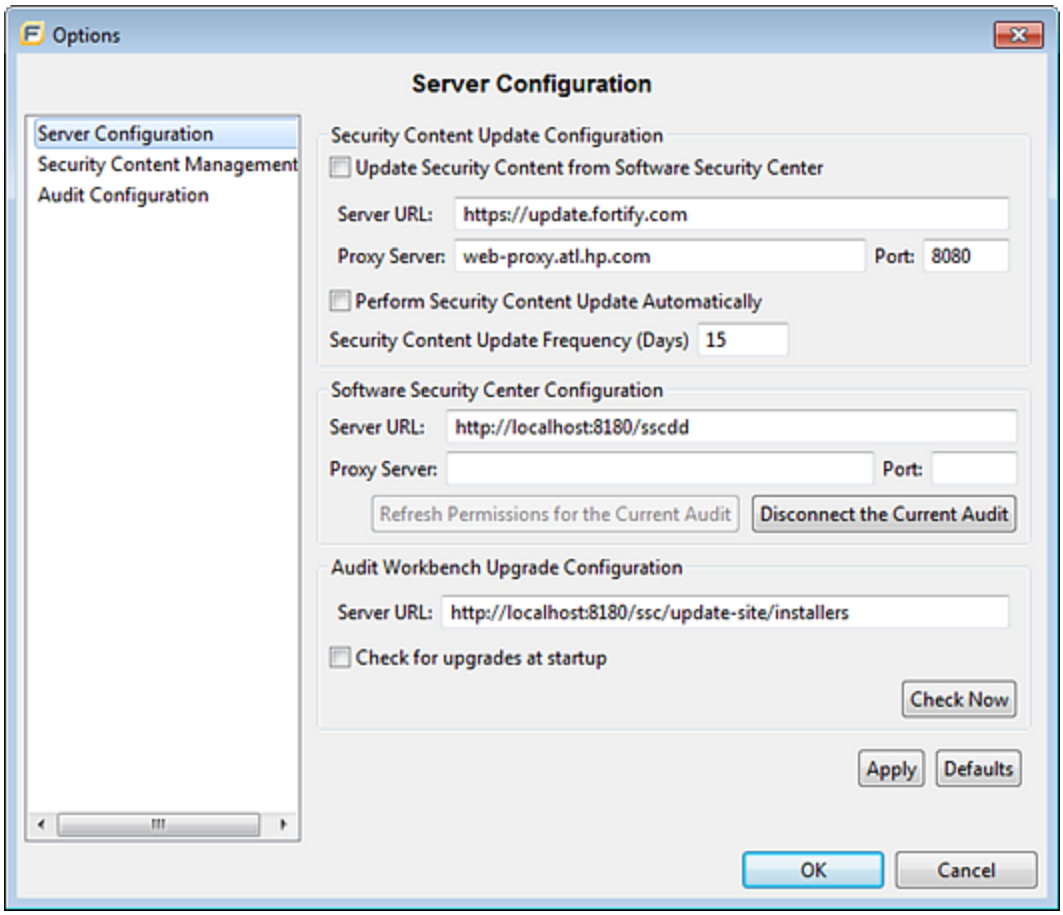
You can update your security content in English, Spanish, Brazilian Portuguese, Japanese, Korean, Simplified Chinese, or Traditional Chinese. HPE recommends that you periodically update the security content.

Configuring Security Content Updates

You can specify the server information to use to update security content.

To configure security content updates:

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



3. To update security content from your Fortify Software Security Center server:
   a. Under **Security Content Update Configuration**, select the **Update Security Content from Software Security Center** check box.
   b. Under **Software Security Center Configuration**, specify the Fortify Software Security Center server URL and if necessary, the proxy server and port number.
4. To specify an update server from which to update security content, in the **Security Content Update Configuration** section, do the following:

a. In the **Server URL** box, type the URL for the update server.
b. If required, specify the proxy server and port.

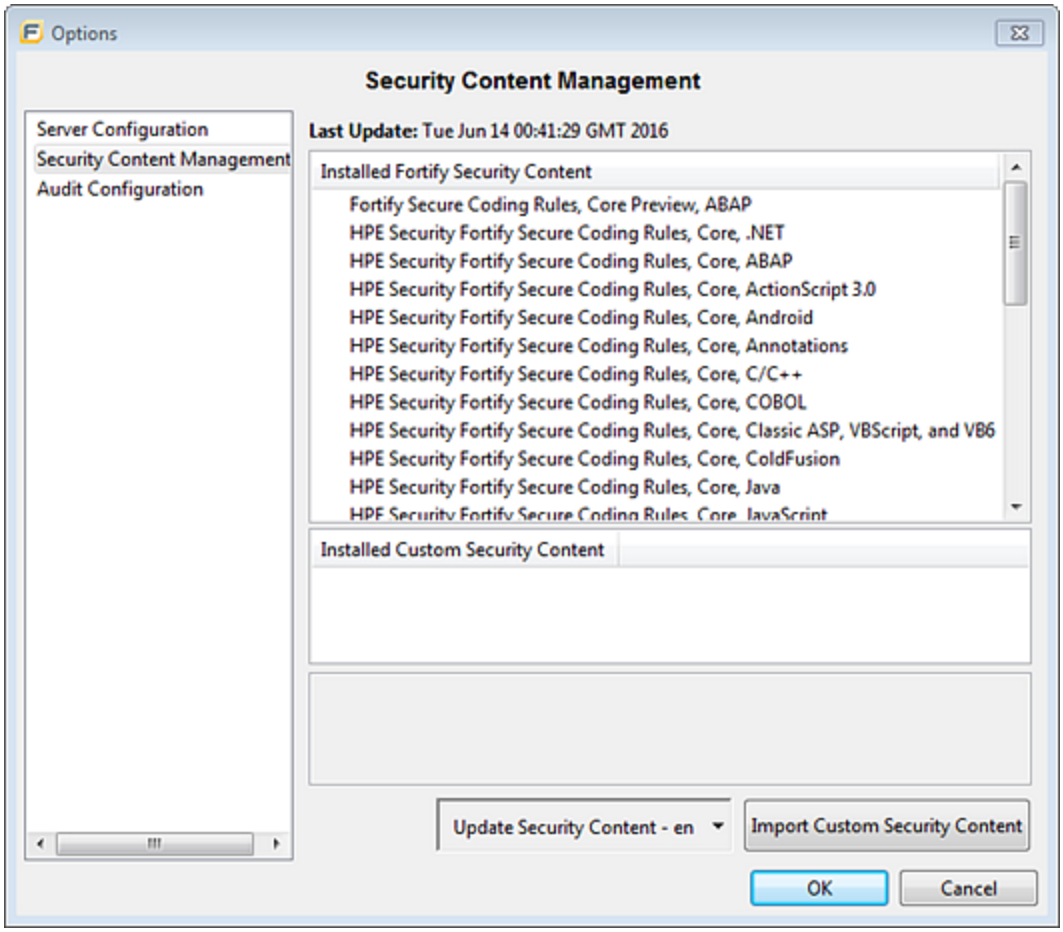
5. To update security content automatically and with a specific frequency:
   a. Select the **Perform Security Content Update Automatically** check box.
   b. In the **Security Content Update Frequency (Days)** box, specify how often (type the number of days) you want the security content automatically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

Updating Security Content

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

To update your security content:

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



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

mappings.

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

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

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

Importing Custom Security Content

To import custom rules, do the following:

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

Logging in to Fortify Software Security Center

The first time you perform an operation that requires a connection to Fortify Software Security Center, you are prompted to log in.

To log in to Fortify Software Security Center:

1. From the **Login Method** menu, select the login method set up for you on Fortify Software Security Center.
2. Depending on the selected login method, do one of the following:

Login Method	Procedure
Username/Password	• Type your Fortify Software Security Center user name and password.
X.509 SSO	a. Click the **Browse** button to the right of **Certificate**. b. In the Browser for Certificate dialog box, locate the p12 package with the certificate, and then click **Open**. c. Type the password if required.
Kerberos SSO	No additional information is required.

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

Chapter 3: Scanning Source Code

The following topics describe how to scan source code and view the scan and analysis results in the Audit Workbench auditing interface.

This section contains the following topics:

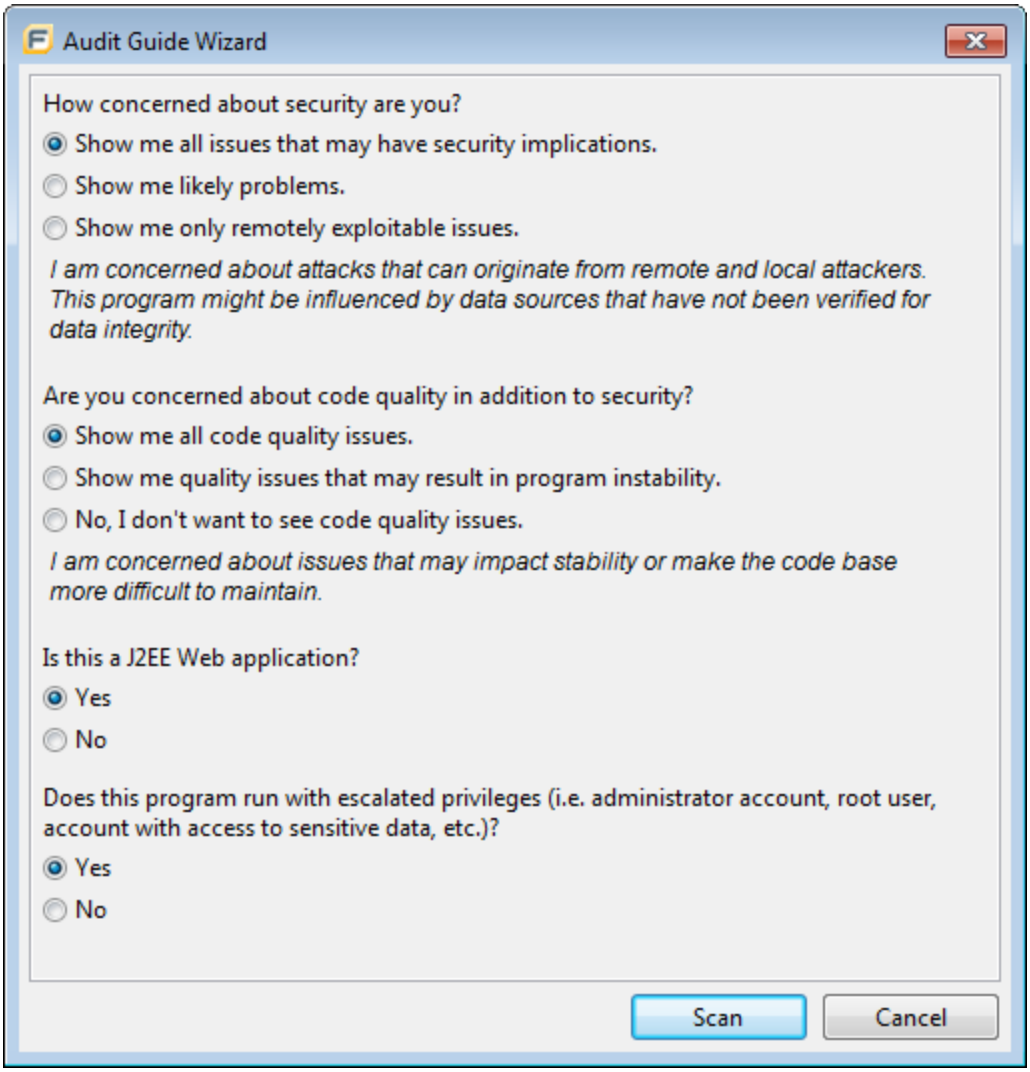
Scanning Java Projects

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 Audit Workbench.
2. Under **Start New Project**, click **Scan Java Project**.
   The Browse for Folder dialog box opens.
3. Select the folder that contains all the source code you want to analyze, and then click **OK**.

   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.



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, Audit Workbench displays a warning.
6. If a warning is displayed, click **OK**.

After the scan is completed, Audit Workbench displays the analysis results.

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

Quick Scan Mode

With quick scan mode, you can quickly scan projects for major issues. For example, a quick scan of the WebGoat sample application uncovers 284 possible issues. By contrast, a full scan of the WebGoat sample application uncovers 1,150 possible issues.

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

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 and Projects" on page 30). 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

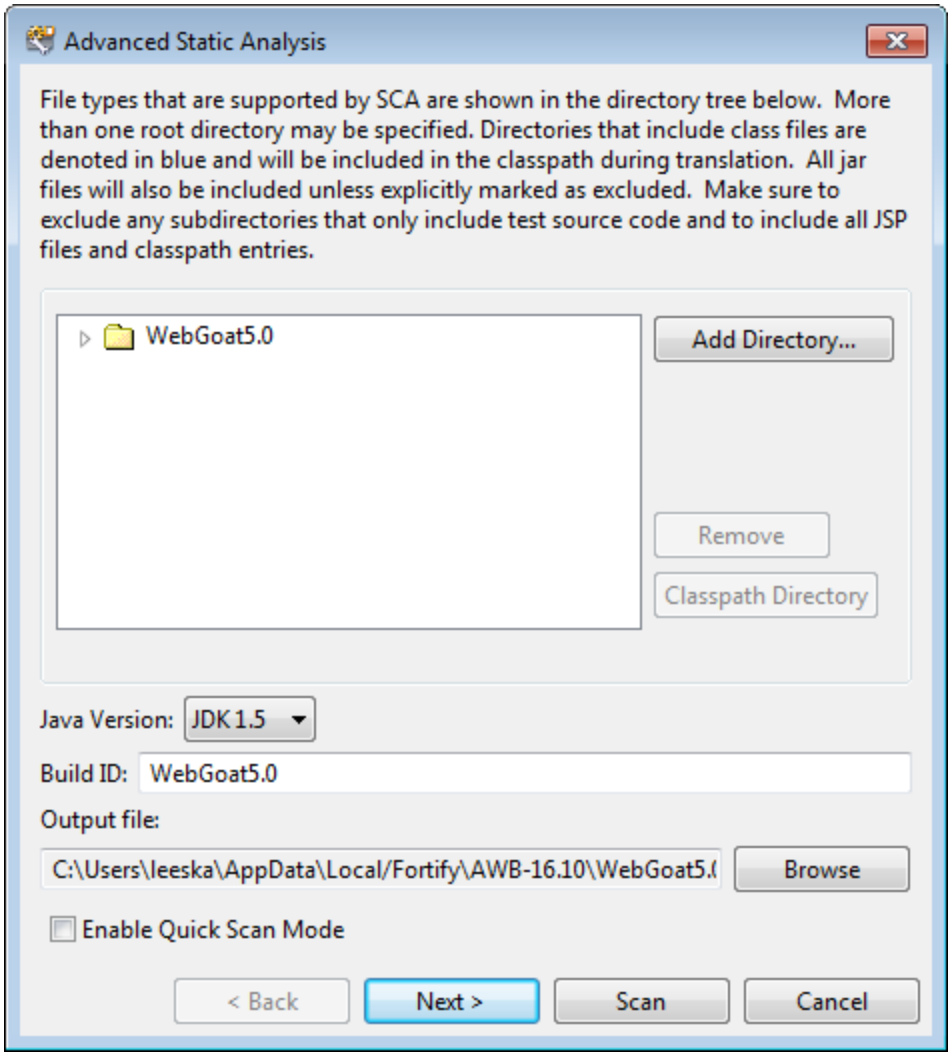
Exceptionally large codebases may require distinct measures to ensure a complete scan, including using Fortify Static Code Analyzer to scan the code in smaller sections. While Audit Workbench enables you to edit Fortify Static Code Analyzer command parameters, you can handle large, complex scans more successfully directly through the command console. In addition, if a system has memory constraints, Fortify Static Code Analyzer must compete with the HPE Security Fortify Audit Workbench for resources, possibly resulting is slow or failed scans.

Use the Advanced Static Analysis wizard to translate and analyze JavaScript, PHP, ASP, .NET, and SQL projects. You can use the wizard for Java projects that have source code in multiple directories, special translation or build conditions, or that have files that you want to exclude from the project.

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

To scan a new project:

1. Start Audit Workbench.
2. Under **Start New Project**, click **Advanced Scan**.
   The Browse for Folder dialog box opens.
3. Select the root directory of the project, and then click **OK**.
   The Advanced Static Analysis wizard opens.



The wizard automatically includes all supported files in the scan.

4. (Optional) To add files from another directory:
   a. Click **Add Directory**.

      The Browse to Folder dialog box opens.
   b. Select the folder that contains the files you want to add to the scan, and then click **OK**.

      The navigation panel displays the directory and 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 select **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 classpath.

b. From the **Java Version** list, select the Java version of the project.

7. In the **Build ID** box, type the build ID.

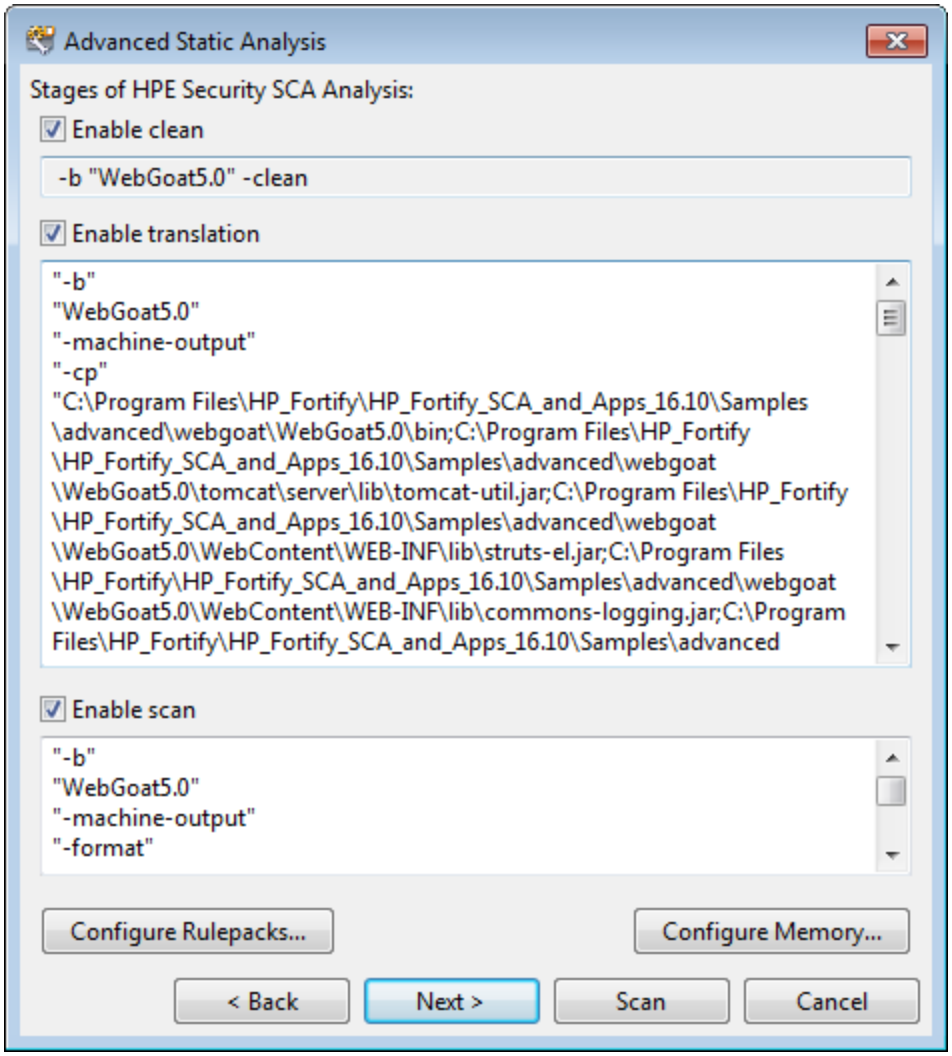
   The root directory is the default build ID.

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 is to generate.

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

   For information about quick scans, see "Quick Scan Mode" on page 24.

10. Click **Next**.



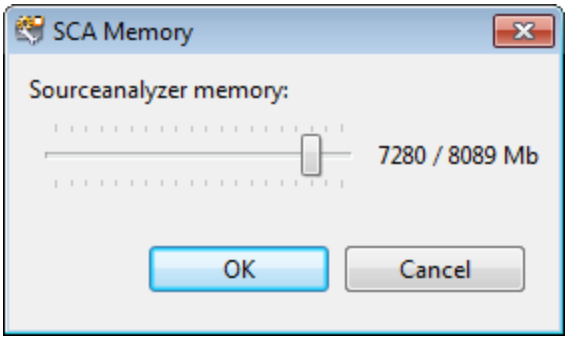
The scan process includes the following phases:

- 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 screen 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 a scanning phase, clear the **Enable clean**, **Enable translation**, or **Enable scan** check box.

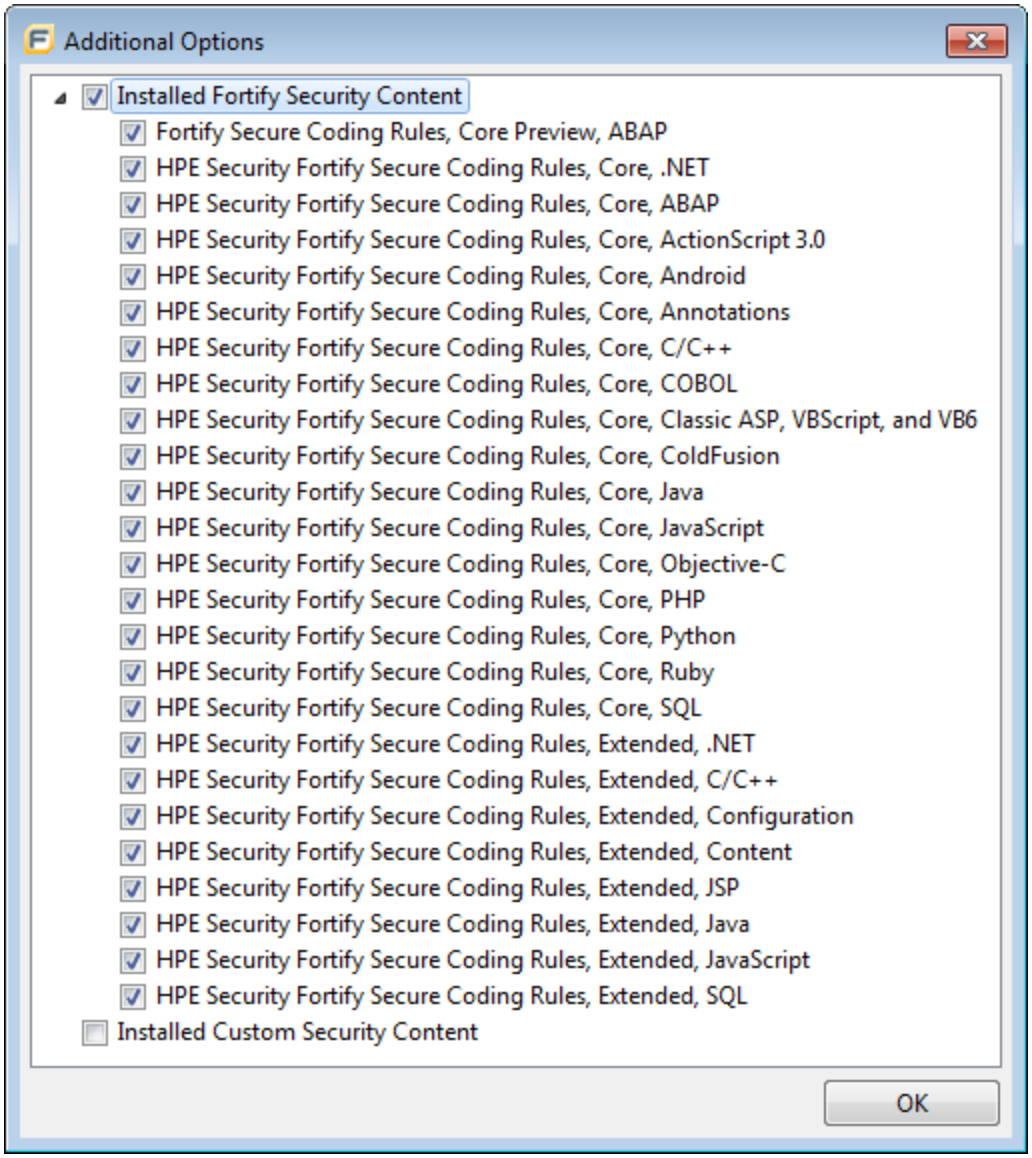
    For example, if the security content has changed but the project has not changed, you might want to disable both the clean and the translation phases so that Fortify Static Code Analyzer scans the project without retranslating.
12. Modify the command-line options for each Fortify Static Code Analyzer scan phase as required.
13. (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.
    c. Click **OK.**

14. (Optional) To analyze the source code using an installed custom Rulepack, or to disable a Rulepack, do the following:
    a. Click **Configure Rulepacks**.

       The Additional Options dialog box opens.

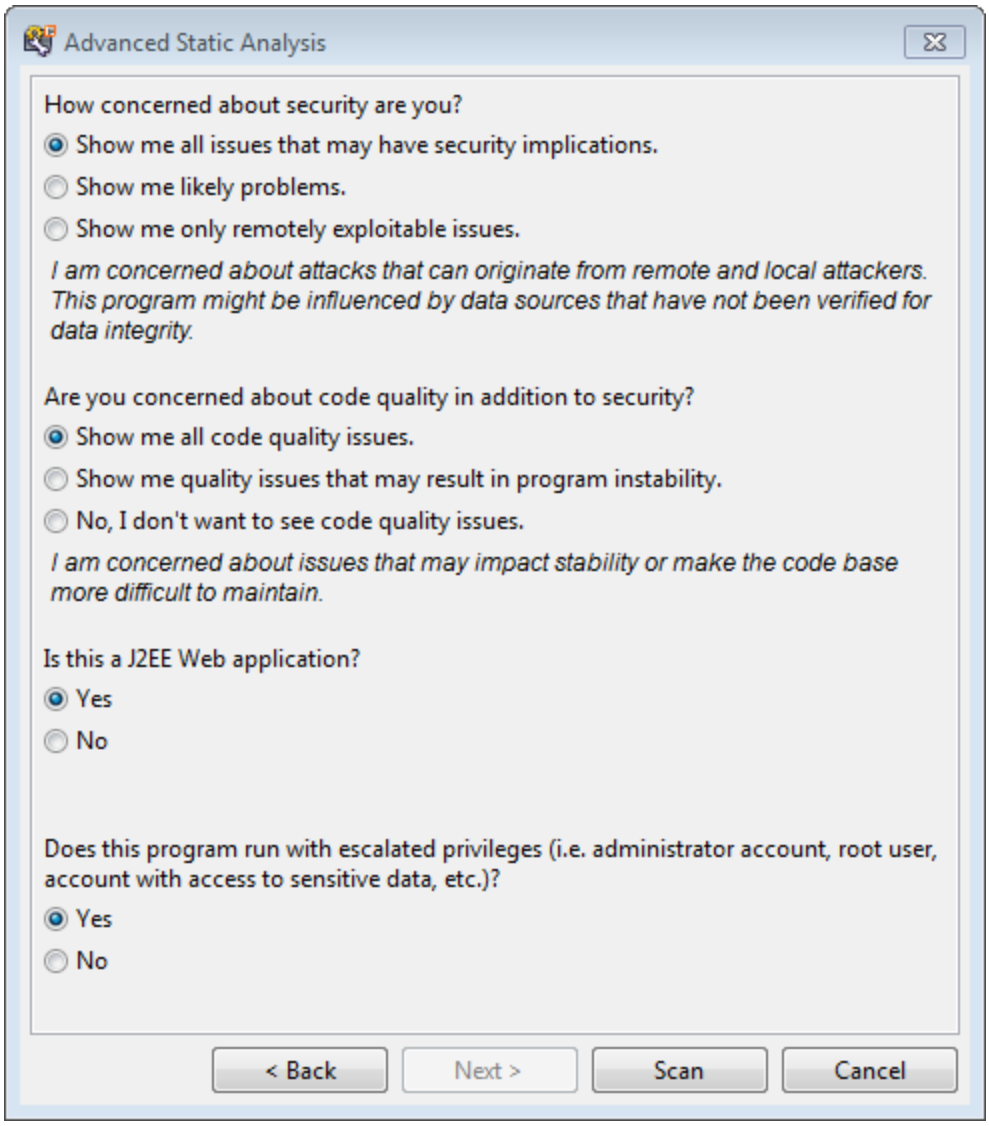


    b. In the **Installed Fortify Security Content** list, clear the check boxes that correspond to any Rulepacks you want to disable during the scan.

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

    c. Click **OK**.

15. From the Advanced Static Analysis wizard, click **Next**.



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 completed, Audit Workbench loads the audit project and displays the analysis results.

Scanning Visual Studio Solutions and Projects

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

The source code analysis supports the following languages in Visual Studio solutions:

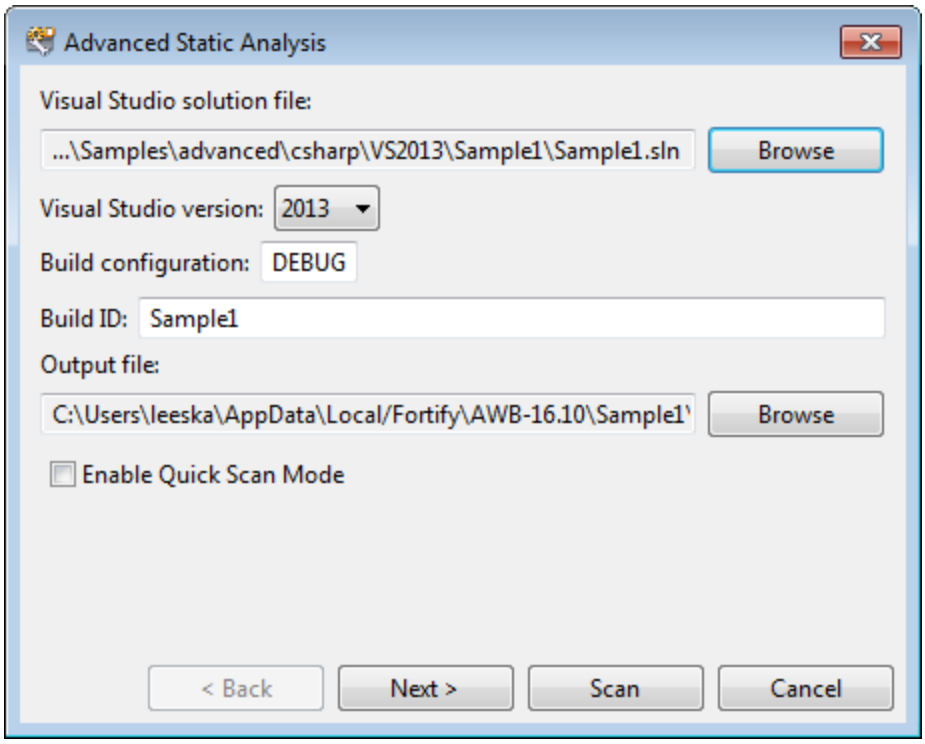
- C/C++
- C#
- VB .NET
- ASP .NET

To scan a Visual Studio solution:

1. Start Audit Workbench.
2. Under **Start New Project**, click **Visual Studio Build Integration**.
3. Select the folder that contains the solution you want to analyze, and then click **OK**.

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

   The Advanced Static Analysis wizard opens.



4. Configure the solution settings, as follows:
   a. (Optional) Next to the **Visual Studio solution file** box, click **Browse**.
   b. Navigate to and select the file for your Visual Studio solution.
   c. From the **Visual Studio version** list, select the Visual Studio version used for the solution.
   d. In the **Build configuration** box, leave the default value DEBUG.
   e. (Optional) In the **Build ID** box, type a different build ID.
   f. (Optional) Select a different path and name for the **Output file**.
   g. To run the scan in quick scan mode, select the **Quick Scan Mode** check box.
   h. 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 screen 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 disable the 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.
   c. Click **OK**.
8. (Optional) To analyze the source code using an installed custom Rulepack, or to disable 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 disable during the scan.

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

   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, Audit Workbench loads the audit project and displays the analysis results.

Re-scanning Projects

This section describes how to re-scan a project that was translated locally with new or updated rules. 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, 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 re-scan a project:

1. Open an FPR file.
2. Click **Scan**.

   Note: You can only re-scan 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 retranslate the project.

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

   Note: If the source code has changed since the most recent scan, you must update the translation before you re-scan 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. (Optional) To change the Rulepacks used to analyze the project:
   a. Click **Configure Rulepacks**.
   b. 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 22.

   c. Click **OK**.
6. Click **Scan**.

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

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

Chapter 4: Scan Results

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

This section contains the following topics:

About Viewing Scan Results

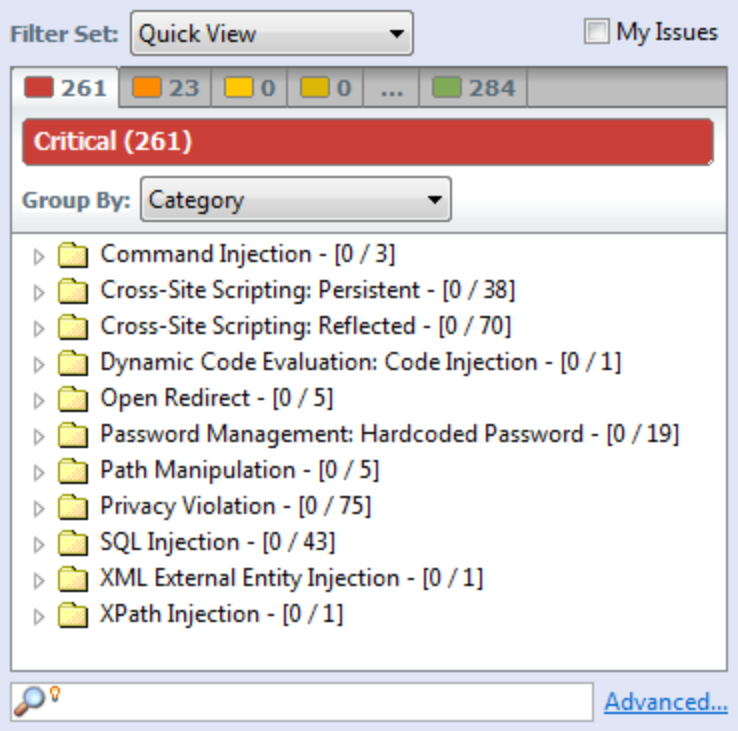
After the scan is completed (or, after you open an existing audit project), summary results are displayed in the **Issues** view and in the **Project Summary** view of the auditing interface. The **Analysis Evidence** and **Issue Auditing** views are open, but do not contain any information until you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

View	For more information, see...
Issues (top left)	"Issues View" below
Project Summary (top center)	"Project Summary View" on page 39
Analysis Evidence (bottom left)	"Analysis Evidence View" on page 38
Issue Auditing (bottom center)	"Issue Auditing View" on page 45
Functions (right)	"Functions View" on page 51

Issues View

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

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



Filter Sets

Audit Workbench applies filters to sort and display the issues that Static Code Analyzer uncovers. 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.

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 reveals a broad set of security issues to be audited. 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 67.

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

Specifying the Default Filter Set

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

To select the filter set for new or opened projects:

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

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

Folders (Tabs)

The color-coded **Critical**, **High**, **Medium**, **Low**, and **All** tabs on the **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 icons in the issues list.

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

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

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

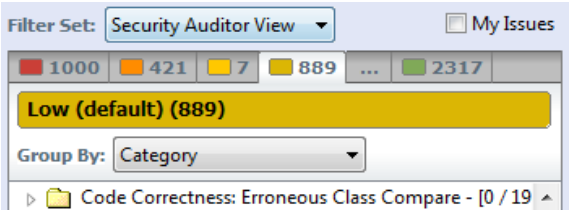
  Example: `Password Management: Hardcoded Password`
- The **Medium** folder contains issues that a have low impact and a high likelihood of exploitation. Medium-priority issues are easy to discover and exploit, but often result in little asset damage. These issues represent a moderate security risk to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

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

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

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

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



You can create your own folders as you need them. For example, you might group all hot issues for a project into a **Hot** folder and group all warning issues for the same project into a **Warning** folder. For instructions on how to create your own folders, see "Creating a Folder" on page 70.

Each folder contains a list of all of 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 51).

Group By List

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

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

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

For more information, see "Grouping Issues" on page 55.

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 panel, select **Audit Configuration**, and then click the **Configuration** tab on the right.
3. Under **Audit Project Load Mode**, select the **Default Issue Grouping** check box.

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

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

Search Box

The search box enables you to limit the issues displayed in the folder and to search for specific issues. For detailed information about how to use the search box, see "Searching for Issues" on page 60.

Analysis Evidence View

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

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

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

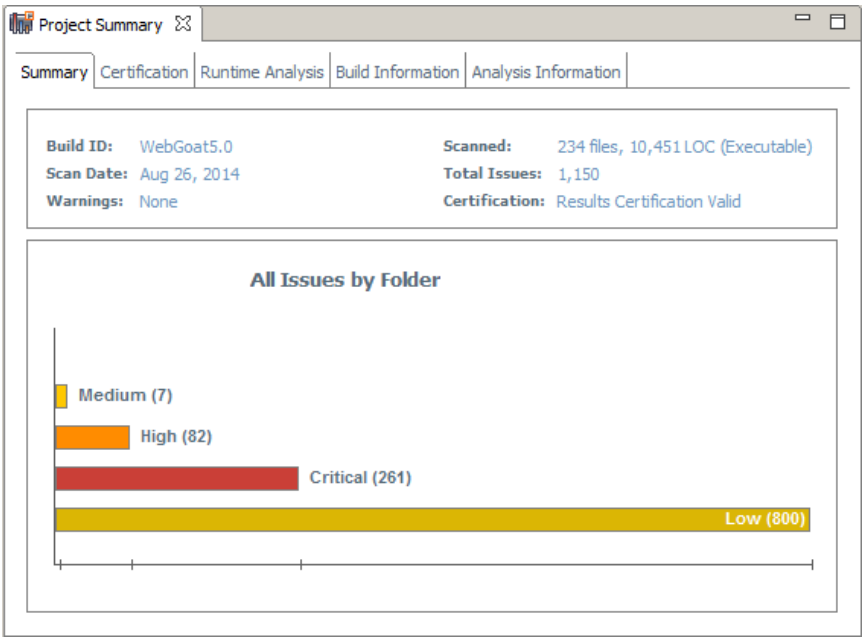
Icon	Description
	Data is assigned to a field or variable
	Information is read from a source external to the code such as an HTML form or a URL
	Data is assigned to a globally scoped field or variable
	A comparison is made
	The function call receives tainted data
	The function call returns tainted data
	Passthrough, tainted data passes from one parameter to another in a function call
	An alias is created for a memory location
	Data is read from a variable
	Data is read from a global variable
	Tainted data is returned from a function

Icon	Description
	A pointer is created
	A pointer is dereferenced
	The scope of a variable ends
	The execution jumps
	A branch is taken in the code execution
	A branch is not taken in the code execution
	Generic
	A runtime source, sink, or validation step
	Taint change

The Analysis Evidence view can display inductions. Inductions provide supporting evidence for their parent nodes. Inductions consist of a text node, displayed in italics as a child of the trace node, and an induction trace, displayed as a child of the text node (a box surrounds the induction trace). The italics and the box distinguish the induction from a standard sub trace.

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.

Certification Tab

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

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

Runtime Analysis Tab

If Runtime analysis data is available, the **Runtime Analysis** tab displays the following run information:

- Number of issues found by Runtime Application Protection
- Build ID
- Engine version
- Dates and times the run started and ended
- Machine on which the scan was performed

Build Information Tab

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

- Build details such as the build ID, number of files scanned, source last-modified date, and the date of the scan, which might be different than the date the files were translated
- Executable lines of code (LOC) scanned - Ignore this metric. It is no longer used.
- Total lines of code (LOC) scanned

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

Analysis Information Tab

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

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

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

Viewing Summary Graph Information

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

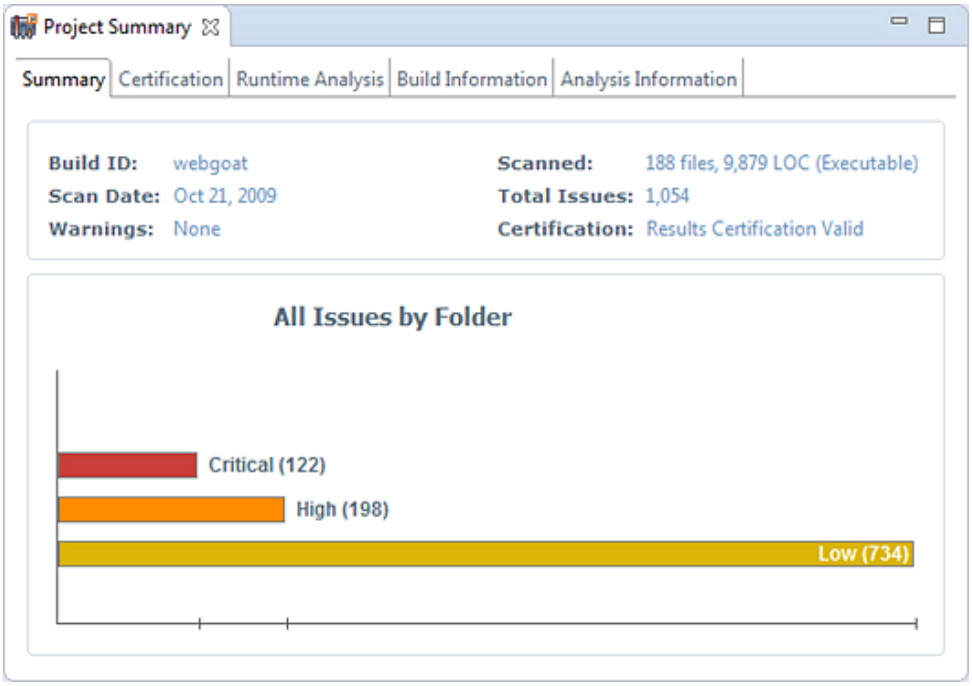
The following procedure uses the WebGoat sample Java application to demonstrate how to access information about sets of issues graphically depicted in the summary graph.

To access details about issue sets in an audit project:

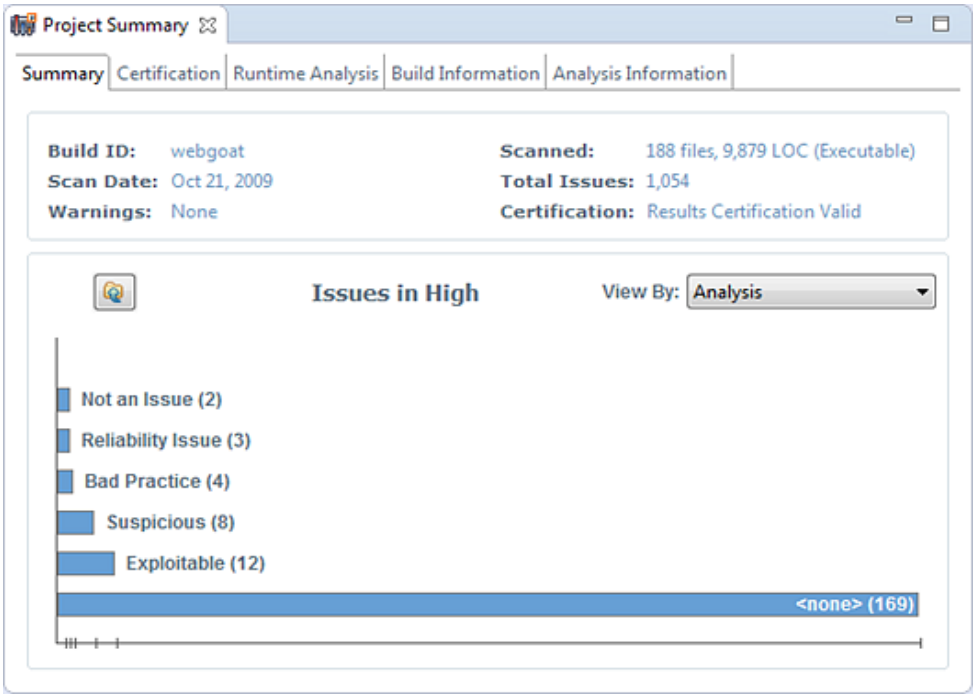
1. Scan your project source code or open an existing audit project.

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

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



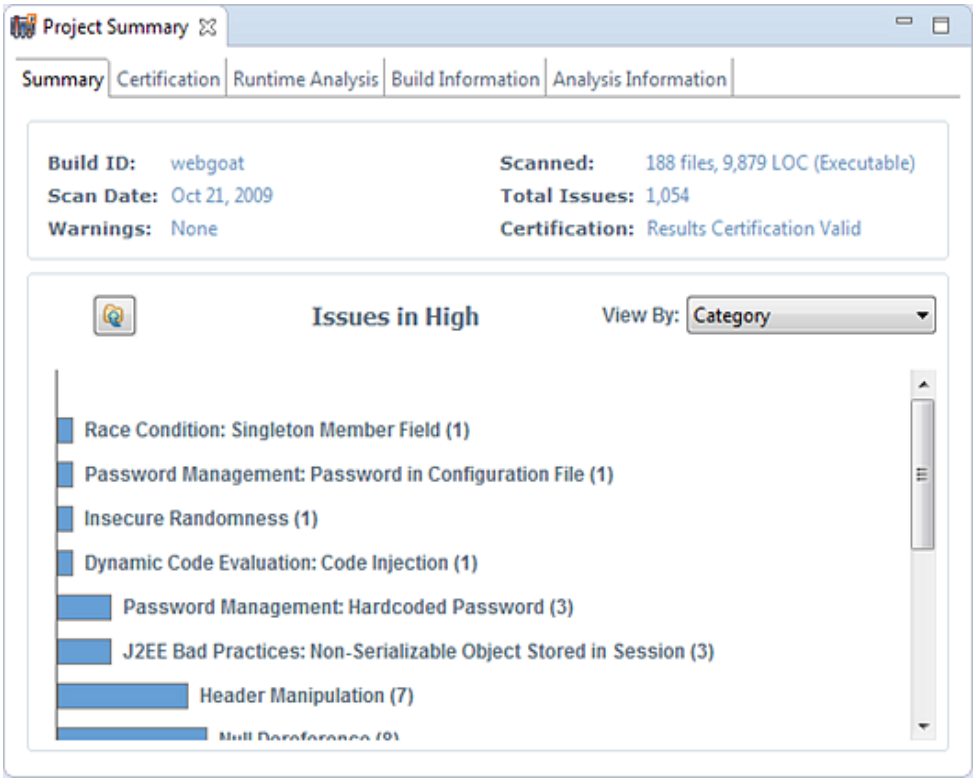
2. To see a different view of the high priority issues, click the **High** bar.



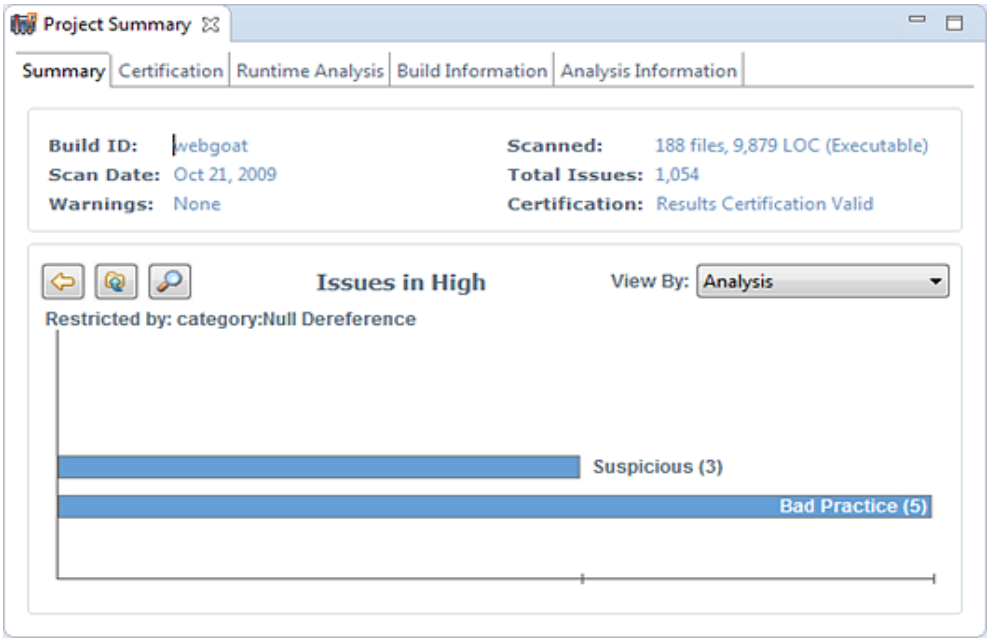
By default, the graph displays high priority issues based on the analysis attribute (assigned analysis values).

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

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

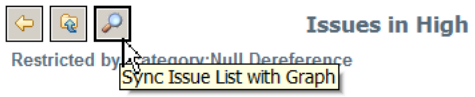


4. On the **Issues in High** bar graph, select a bar for a category that contains multiple issues.



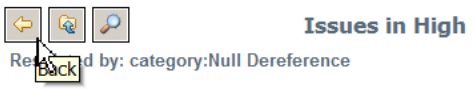
In the example shown here, the **Null Dereference** bar is selected. You can see that, of eight issues, three were marked as Suspicious and five were marked as Bad Practice.

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

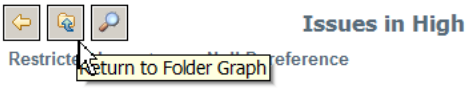


The issues list in the **Issues** view now reflects the selections in the summary graph.

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 View

After you open a project in Audit Workbench, the top center view displays the **Project Summary** tab. After you select an issue in the **Issues** view to the left, 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 Evidence** view (below the **Issues** view), the source code tab shows the code associated with the selected node. From the source code view, you can use the code assist feature to create custom rules and new issues. For information about how to create a new issue from Audit Workbench, see "Creating Issues for Undetected Vulnerabilities" on page 87.

About Displayed Source Code

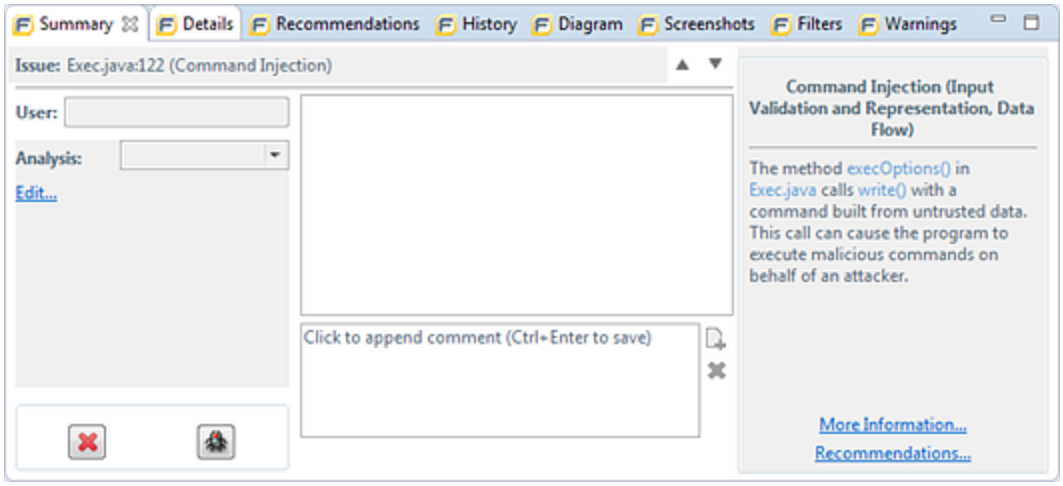
After you open an FPR file in Audit Workbench, the source code tab displays source code that is stored locally. If that source code was updated since the last scan, Audit Workbench displays the updated source code, even if the latest scan did not use that updated source code.

However, if that source code is updated after you open the FPR file and 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) 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 Audit Workbench.

Issue Auditing View

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

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



Summary Tab

The **Summary** tab displays information about the selected issue and enables auditors to add comments and custom tag values. The following table describes the tab elements.

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

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

Details Tab

The **Details** tab provides a detailed description of the selected issue and guidelines on how to resolve it. The following table describes the tab elements.

Element	Description
Abstract/Custom Abstract	Summary description of the issue, including custom abstracts that your organization defined.
Explanation/Custom	Description of the conditions in which this type of issue occurs. This includes a

Element	Description
Explanation	discussion of the vulnerability, the constructs typically associated with it, how it can be exploited, and the potential consequences of an attack. This element also provides custom explanations that your organization defined.
Instance ID	Unique identifier for the issue.
Priority Metadata Values	Includes impact and likelihood.
Legacy Priority Metadata Values	Includes severity and confidence.
Remediation Effort	The relative amount of effort required to fix and verify an issue.

Note: For more information about metadata values and remediation effort, see "Estimating Impact and Likelihood with Input from Rules and Analysis" on page 122.

WebInspect Agent Details Tab

The **WebInspect Agent Details** tab displays the following information about runtime issues found by HPE Security Fortify Runtime Application Protection. The following table describes the tab elements.

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

Recommendations Tab

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

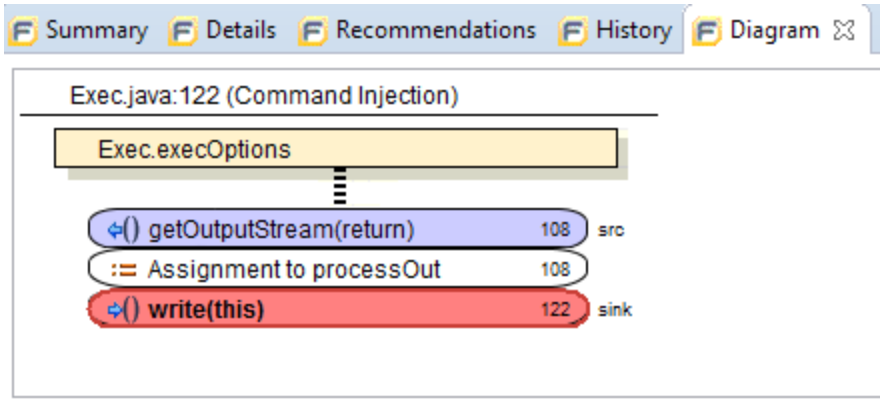
Element	Description
Recommendations/Custom Recommendations	Recommendations for this type of issue, including examples, as well as custom recommendations that your organization defined.
Tips/Custom Tips	Tips for this type of issue, including any custom tips that your organization defined.
References/Custom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

History Tab

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

Diagram Tab

The **Diagram** tab displays a graphical representation of the node execution order, call depth, and expression type of the issue selected in the **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 it 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 Evidence** view. To view the icons and the descriptions, see "Analysis Evidence View" on page 38.

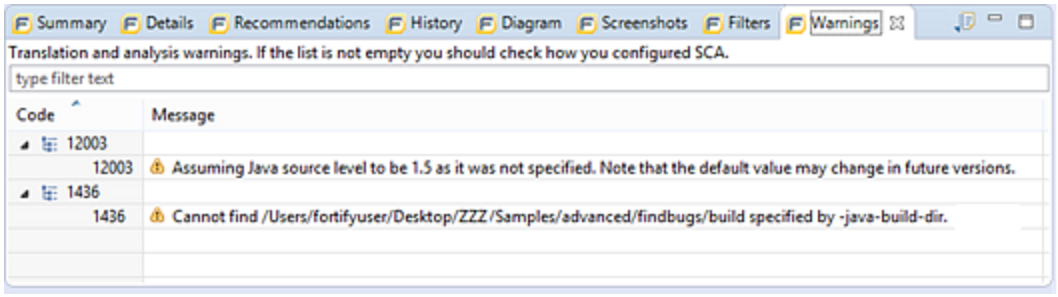
Filters Tab

The **Filters** tab displays all the filters in the selected filter set. The following table describes the **Filters** tab options to create new filters.

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

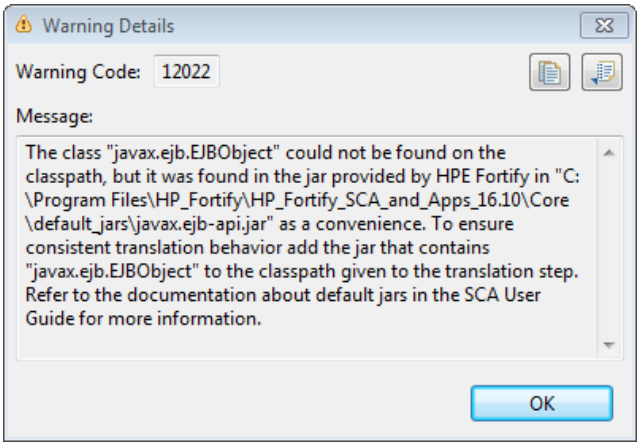
Warnings Tab

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 particular class has no functional content. In this case, the warning is not an issue because an empty class has no impact on a scan.

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

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

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

Functions View

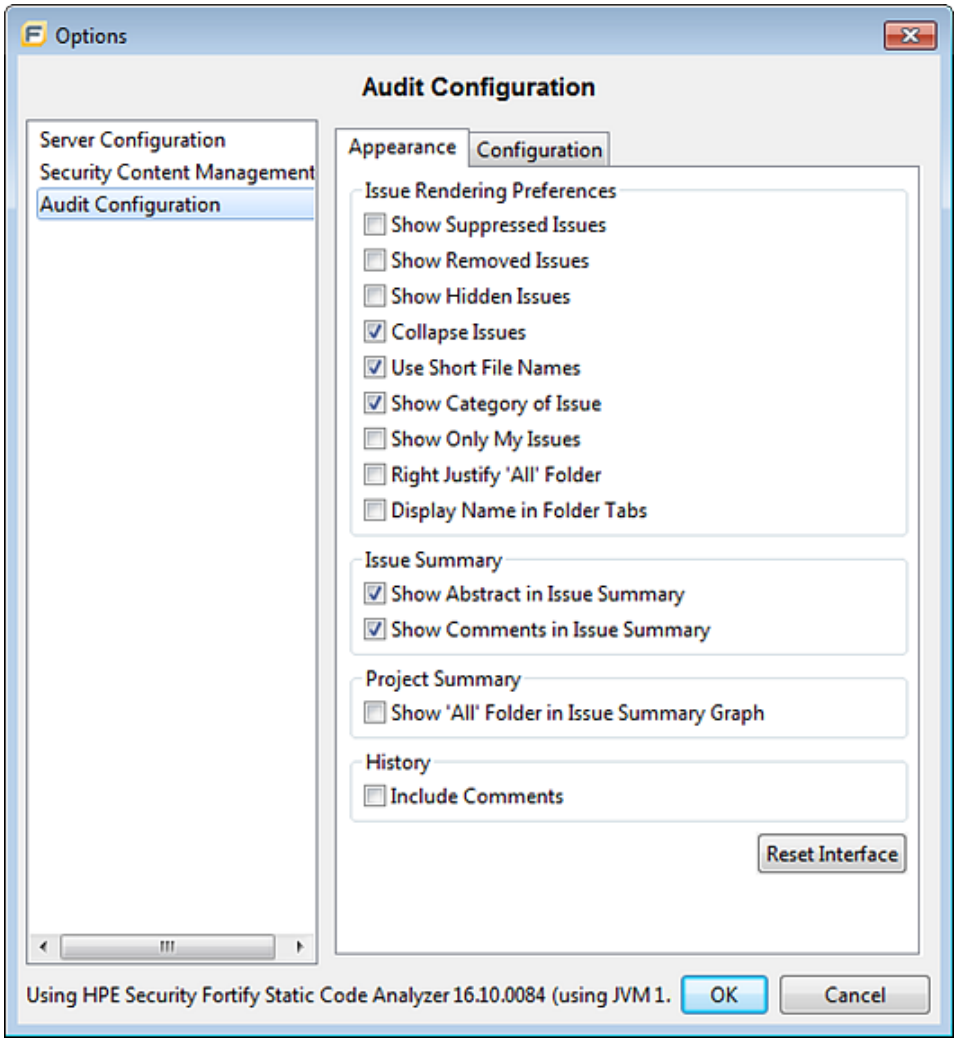
The **Functions** view in the top right shows how and where a function occurs in the source code, whether or not the function was covered by a security rule, and which rule IDs match the function. The **Functions** view can also list the functions that Fortify Static Code Analyzer identified as tainted 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 106.

Customizing the Issues View

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

To change the **Issues** view:

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



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

Preference	Description
Show Suppressed Issues	Displays all suppressed issues (disabled by default).
Show Removed Issues	Displays all issues that were uncovered in the previous analysis, but are no longer evident in the new **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.
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.

Preference	Description
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** and **Issue Summary** views.
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 in Issue Summary	Displays the abstract text in the summary.
Show Comments in Issue Summary	Displays comments in the summary.
Show 'All' Folder in Issue Summary Graph	Displays another bar in the chart on the **Project Summary** tab.
Include Comments	Displays the history items for comments on the **History** tab.

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

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

Working with Issues

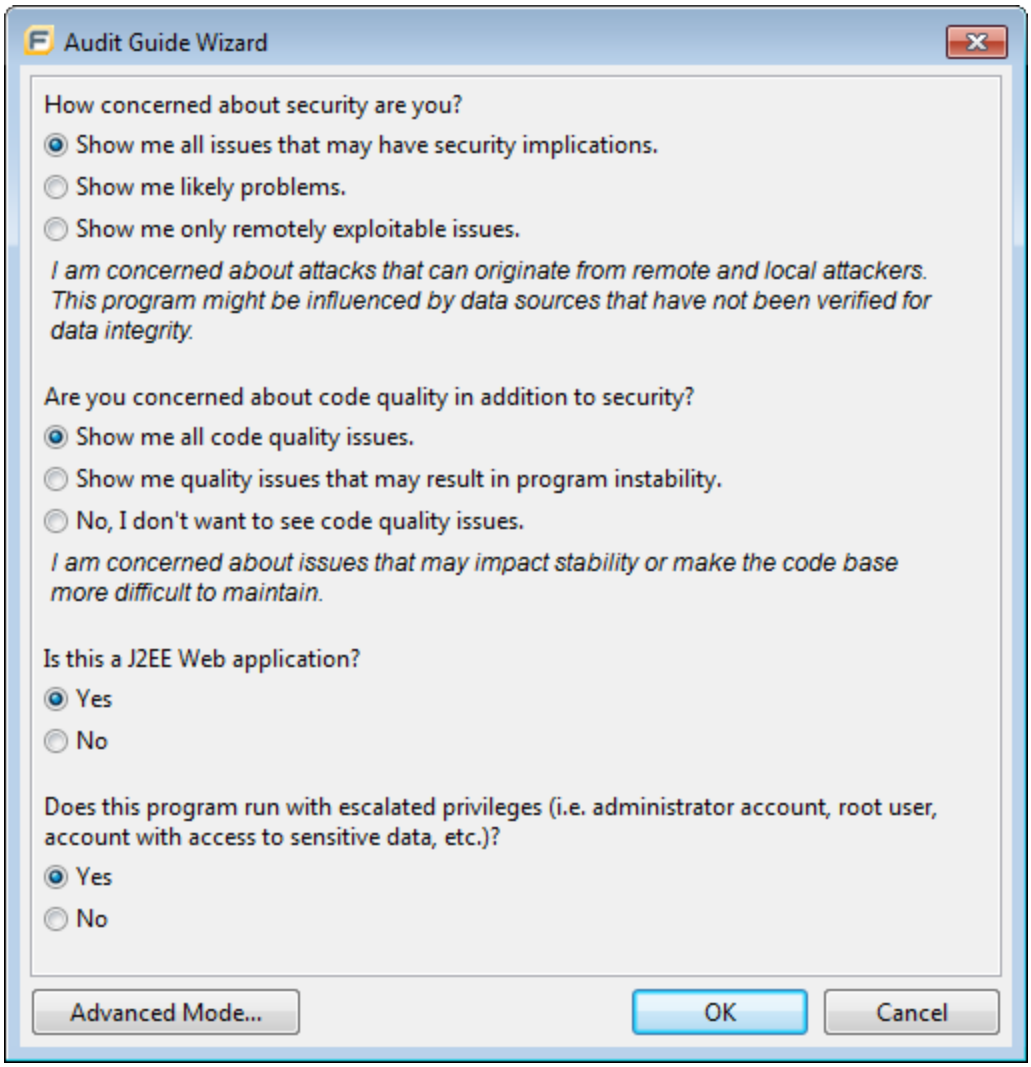
This section provides information about how to use Audit Workbench to review issues.

Filtering Issues with Audit Guide

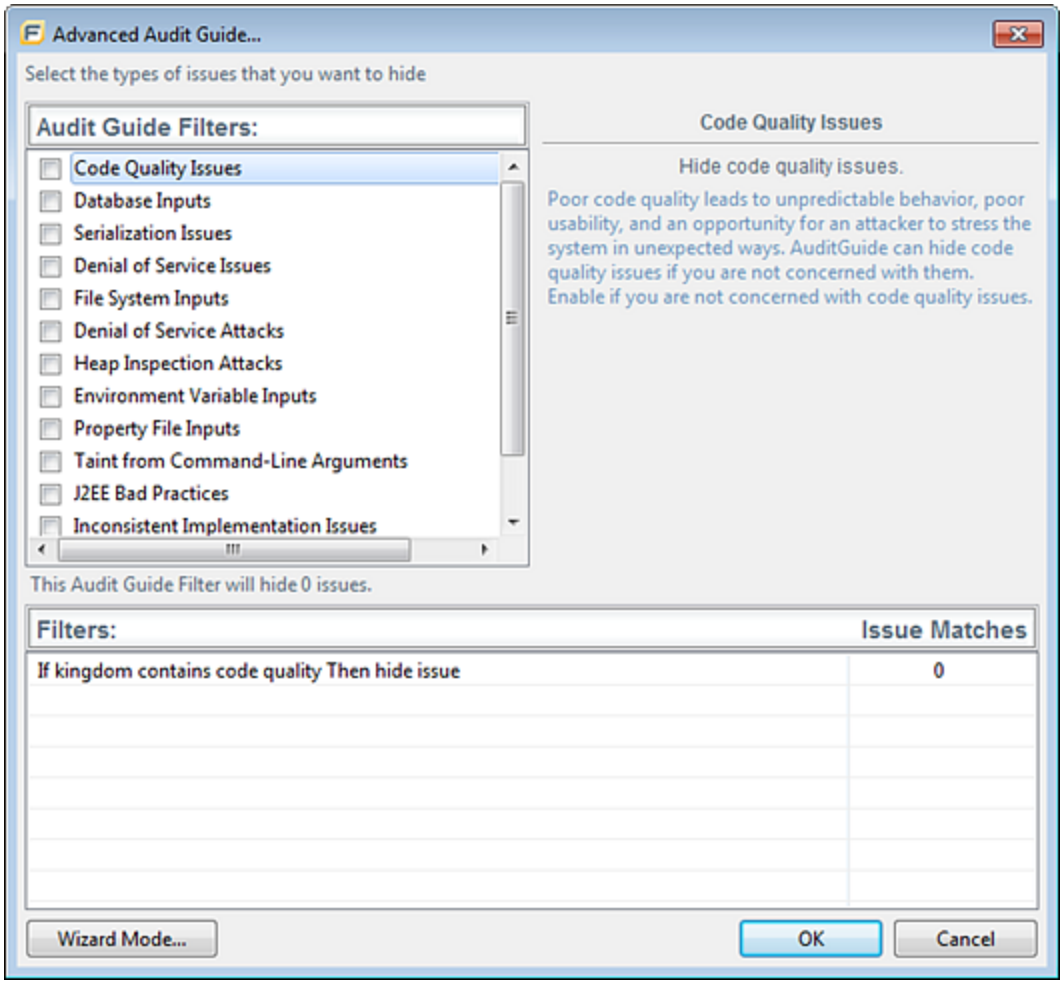
You can use the Audit Guide wizard to filter vulnerability issues in your audit project based on a set of security-related questions.

To use the Audit Guide:

1. Select **Tools > Audit Guide**.



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



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

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

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

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

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

Grouping Issues

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

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

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

Option	Description
Analysis	Groups issues by the audit analysis, such as suspicious and exploitable.
Analysis Type	Groups issues by analyzer product.
Analyzer	Groups issues by analyzer group.
App Defender Protected	Groups issues by whether or not Application Defender can protect the vulnerability category.
Category	Groups issues by vulnerability category. This is the default setting.
Category Analyzer	A sample custom group that groups issues by category and then analyzer.
File Name	Groups issues by file name.
Fortify Priority Order	Groups issues as Critical, High, Medium, and Low based on the combined values of Fortify Static Code Analyzer impact and likelihood.
New Issue	Shows which issues are new since the last scan. For example, if you run a new scan, any issues that are new display in the tree under the **New Issues** group and the others are displayed in the **Issue Updated** group. Issues not found in the latest scan are displayed in the **Removed** list.
<*metadata_listname*>	Groups issues by the alternative metadata external list names (for example, OWASP Top 10 <*year*>, CWE, PCI <*version*>, STIG <*version*>, and so on).
Package	Groups issues by package or namespace. Does not appear for projects to which this option does not apply, such as C projects.
Sink	Groups issues that share the same dataflow sink function.
Source	Groups issues that share the same dataflow source functions.
Source File Type	Groups issues by source file types Fortify Static Code Analyzer recognizes. **Note:** Issues in files with different file extensions that are the same source file type are grouped together (for example, issues in files with the extensions: `html`, `htm`, and `xhtml` are grouped under html).
Taint Flag	Groups issues by the taint flags that they contain.
<none>	Displays a flat view without grouping.
Edit	Select **Edit** to create a custom Group By option.

Creating a Custom Group By Option

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

To create a new grouping option:

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

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

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

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

Selectively Displaying Issues Assigned to You

To view 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 might not be 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 could 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 deselect) 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 panel, select **Audit Configuration**, and then select the **Configuration** tab.
3. Under **Multiple Issues Copy Format**, leave the **[h] List issues in columns** option selected.
4. Select the attributes you want to include from the **Include immutable attributes**, **Include mutable attributes**, and **Include custom tags** check boxes.
5. Click **OK**.
6. From the **Issues** view, use the **Ctrl** or **Shift** key and select all of 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 panel, select **Audit Configuration**, and then select the **Configuration** tab.
3. Under **Multiple Issues Copy Format**, select the **[v] List issues in rows** option.
4. Select the attributes you want to include from the **Include immutable attributes**, **Include mutable attributes**, and **Include custom tags** check boxes.
5. Click **OK**.
6. From the **Issues** view, use the **Ctrl** or **Shift** key and select all of 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 panel, select **Audit Configuration**, and then select the **Configuration** tab.
3. Under **Multiple Issues Copy Format**, select the **Format manually** option.
4. In the **Attribute value format** box, use the string described in the following table to specify the data layout, format, and separators for the values you want to copy.

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

Searching for Issues

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

You can wrap search terms with delimiters to indicate the type of comparison to be performed. The following table shows the syntax to use in the search string field.

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]` means 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>`. For more information, see "Search Modifiers" on the next page.

A search string can contain multiple modifiers and search terms. If you specify more than one modifier, the search returns only issues that match all the modified search terms. For example, `file:ApplicationContext.java category:SQL Injection` returns only SQL injection issues found in `ApplicationContext.java`.

If you use the same modifier more than once in a search string, then the search terms qualified by those modifiers are treated as an `OR` comparison. For example, `file:ApplicationContext.java`

`category:SQL Injection category:Cross-Site Scripting` returns SQL injection issues and cross-site scripting issues found in `ApplicationContext.java`.

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

For more information, see "Search Modifiers" below.

Search Modifiers

You can use a search modifier to specify which attribute of an issue the search term applies to. 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, enter `[issue age]:new`.

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

- To apply the search to all modifiers, enter a string such as `control flow`. This searches all of the modifiers and returns any result that contains the specified string.
- To apply the search to a specific modifier, type the modifier name and the string as follows: `analyzer:control flow`. This returns all results whose analyzer is `control flow`.

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

Modifier	Description
`analysis`	Searches for issues that have the specified audit analysis value (such as `exploitable`, `not an issue`, and so on).
`analyzer`	Searches the issues for the specified analyzer.
`audience`	Searches for issues based on intended audience. Valid values are `targeted`, `medium`, and `broad`.
`audited`	Searches the issues to find `true` if the primary custom tag is set and `false` if the primary custom tag is not set. The default primary tag is the Analysis tag.
`category(cat)`	Searches for the given category or category substring.
`comments (comment, com)`	Searches for issues that contain the search term in the comments that have been submitted on the issue.
`commentuser`	Searches for issues with comments from a specified user.
`confidence (con)`	Searches for issues that have the specified confidence value. Fortify Static Code Analyzer calculates the confidence value based on the number of assumptions made in code analysis. The more assumptions made, the lower the confidence value.

Modifier	Description
`dynamic`	Searches for issues that have the specified dynamic hot spot ranking value.
`file`	Searches for issues where the primary location or sink node function call occurs in the specified file.
`[fortify priority order]`	Searches for issues that have a priority level that matches the specified priority determined by Fortify Static Code Analyzer. Valid values are `critical`, `high`, `medium`, and `low`, based on the expected *impact* and *likelihood* of exploitation. The impact value indicates the potential damage that might result if an issue is successfully exploited. The likelihood value is a combination of confidence, accuracy of the rule, and probability that the issue can be exploited.
`historyuser`	Searches for issues that have audit data modified by the specified user.
`[issue age]`	Searches for the issue age, which is `new`, `updated`, `reintroduced`, or `removed`.
`kingdom`	Searches for all issues in the specified kingdom.
`maxconf`	Searches for all issues that have a confidence value equal to or less than the number specified as the search term.
`minconf`	Searches for all issues that have a 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.
`[primary context]`	Searches for issues where the primary location or sink node function call occurs in the specified code context. Also see sink and [source context].
`primaryrule (rule)`	Searches for all issues related to the specified sink rule.
`ruleid`	Searches for all issues reported by the specified rule IDs used to generate the issue source, sink and all passthroughs.
`sink`	Searches for issues that have the specified sink function name. Also see [primary context].
`source`	Searches for dataflow issues that have the specified source function name. Also see [source context].
`[source context]`	Searches for dataflow issues that have the source function call contained in the specified code context.

Modifier	Description
	Also see source and [primary context].
`sourcefile`	Searches for dataflow issues with the source function call that the specified file contains. Also see file.
`status`	Searches issues that have the status reviewed, not reviewed, or under review.
`suppressed`	Searches for suppressed issues.
`taint`	Searches for issues that have the specified taint flag.
`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.
<custom_tagname>	Searches the specified custom tag. You can search a list-type custom tag using a range of values. The values of a list-type custom tag are an enumerated list where the first value is 0, the second is 1, and so on. You can use the search syntax for a range of numbers to search for ranges of list-type custom tag values. For example, `analysis:[0,2]` returns the issues that have the values of the first three Analysis values, 0, 1, and 2 (Not an Issue, Reliability Issue, and Bad Practice). To search a date-type custom tag, specify the date in the format: yyyy-MM-dd.
<metadata_listname>	Searches the specified metadata external list. Metadata external lists include `[owasp top 10 2013]`, `[sans top 25 2011]`, `[PCI 3.2]`, and others.

Search Query Examples

The following are search query examples that use search modifiers.

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

- To search for all paths that contain traces with `cleanse` as part of the name, type:
  `trace:cleanse`
- To search for all issues that contain `cleanse` as part of any modifier, type:
  `cleanse`
- To search for all suppressed vulnerabilities with `asdf` in the comments, type:
  `suppressed:true comments:asdf`
- To search for all categories except for SQL Injection, type:
  `category:!SQL Injection`

Performing Simple Searches

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

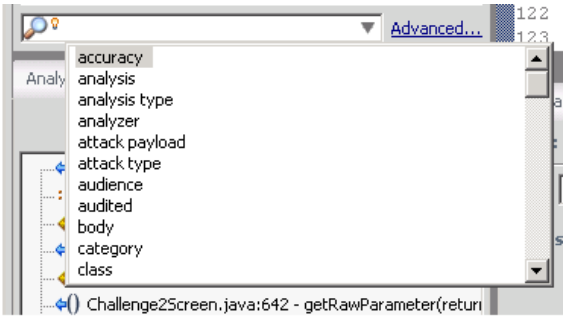
- Type a search string in the box and press **Enter**.

Alternatively,

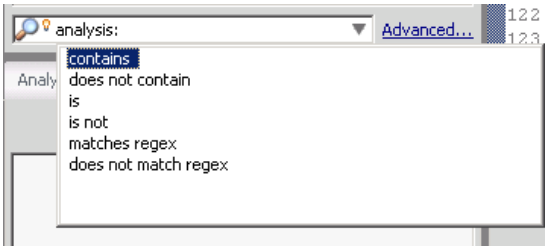
- To select a search term you used previously, click the arrow in the search box, and then select a search term from the list.

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

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



2. From the displayed list, double-click an issue attribute to begin your search string.
3. To get assistance to specify the comparison, with your cursor placed after the modifier in the search box, press **Ctrl** + **Space**.



4. From the displayed list, double-click the comparison to add to your search string.
5. Type the rest of the search term.

The **Issues** view lists all of the issues that match your search string.

Audit Workbench saves all of the search terms you enter for the current session. To select a search term you used previously, click the arrow in the search box, and then select a search term. (After you close Audit Workbench, the saved search terms are discarded.)

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

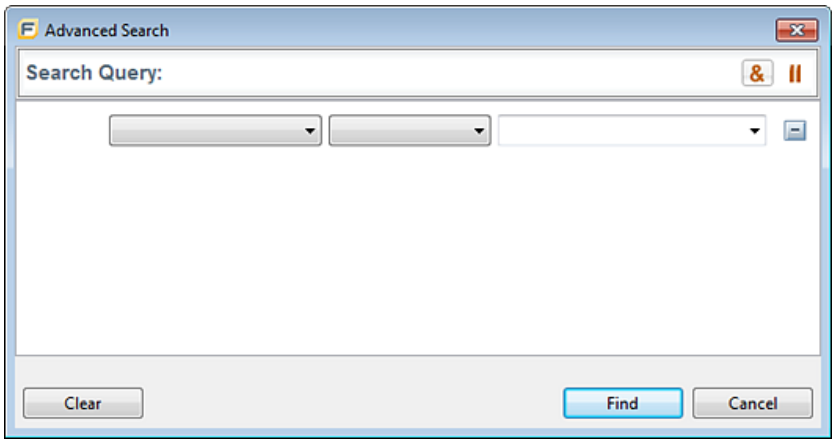
The advanced search feature makes it easier to build complex search strings. For a description of this feature and instructions on how to use it, see "Performing Advanced Searches" below.

Performing Advanced Searches

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

To use the advanced search feature:

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



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

   The list for the search term includes the known values in the current scan for the specified attribute. However, you can type any value into this field. To specify an unqualified search term, select **Any Attribute** from the bottom of the modifier list.
3. To add another query row, do one of the following:
   - To add an AND query row, in the top right corner of the dialog box, click **AND** &.
   - To add an OR query row, in the top right corner of the dialog box, click **OR** ||.
4. Add as many query rows as you need for the search.
5. To delete a row, to the right of the row, click **Delete** −. To remove all rows, click **Clear**.
6. Click **Find**.

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

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 users different views, and a customized view does not affect any other views.

In addition to providing sorting and filtering mechanisms, you can also customize the auditing process by defining custom tags in the issue template. Auditors associate custom tags with issues during auditing. For example, custom tags can be used 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 defect tracking system.

Issue templates contain the following settings:

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

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

1. Template that exists in the audit project
2. Template in `<sca_install_dir>/Core/config/filters/defaulttemplate.xml`
3. Template in `<sca_install_dir>/Core/config/rules/defaulttemplate.xml` or `projecttemplate.xml`
4. Embedded HPE Security 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 on 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 79 and "Synchronizing Filter Sets and Folders" on page 78.

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

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

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

Creating a Filter from the 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 **CreateFilter**.

   The Create Filter dialog box lists suggested conditions.
3. To see all of the conditions, select the **Show all conditions** check box.
4. Select the conditions you want to use in the filter.

   You can fine tune the filter later by modifying it on the **Filter** tab.
5. Select the type of filter you want to create, as follows:
   - To create a visibility filter, select **Hide Issue**.
   - To create a folder filter, select **Set Folder to**, and then select the folder name or select **Other Folder** to add an existing folder or create a new one.

     A new folder is displayed in this filter set only.
6. Click **Create Filter**.

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

The issues are sorted with the new filter.

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

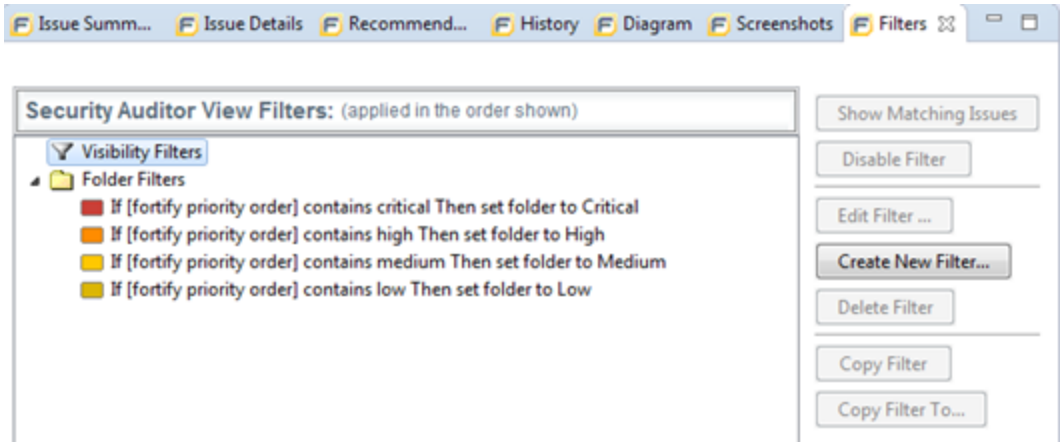
Creating a Filter from the Issue Auditing View

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

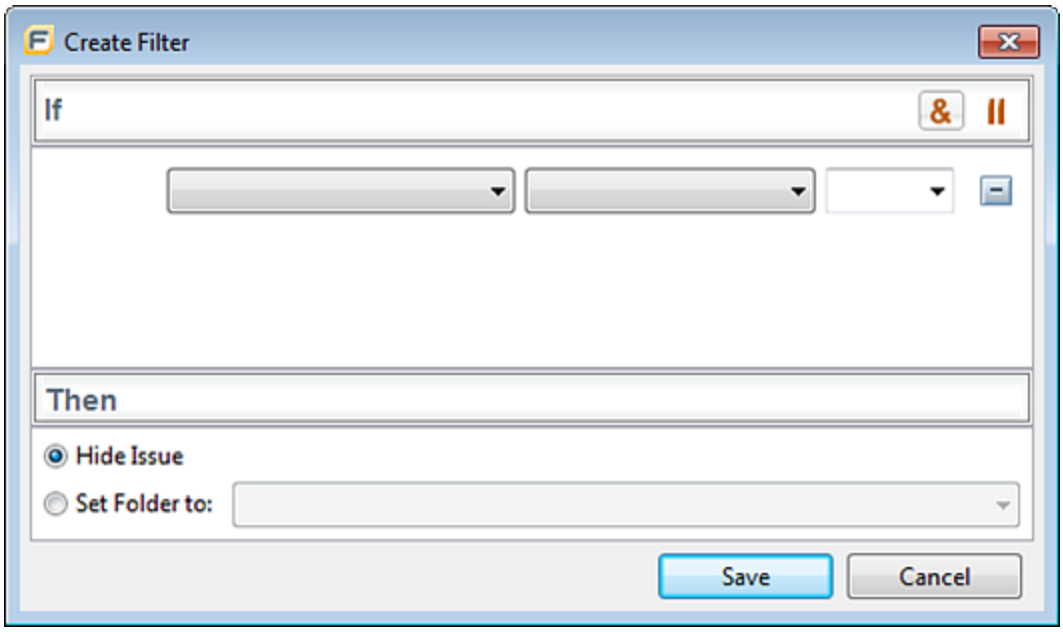
Folder filters are applied in order and the issue is directed to the last folder filter it matches in the list.

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

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



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



4. From the first list, select an issue attribute.
   The second list is automatically populated.
5. From the second list, select how to match the value.
   The third list contains the possible values for the attribute.
6. Select a value or specify a range as instructed in the **If** line.
7. Set **Then** to one of the following options:
   - To create a visibility filter, select **Hide Issue**.
   - To create a folder filter, select **Set Folder to**, and then select the folder name or select **Other Folder** to add a folder from another filter set or create a new folder.
8. Click **Save**.
   The new filter is displayed at the end of the list. For folder filters, this gives the new filter the highest priority. Issues that match the new folder filter appear in the targeted folder.
9. (Optional) For folder filters, drag the filter higher in the folder filter list to change the priority.

The issues are sorted with the new filter.

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

Copying a Filter from One Filter Set to Another

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

To copy a filter:

1. In the **Issues** view, select a filter set from the **Filter Set** list.
2. Click the **Filters** tab in the Issue Auditing view.
3. Right-click a filter, and then select **Copy Filter To** from the shortcut menu.
   The Select a Filter Set dialog box opens with a list off 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 intend to provide sorting mechanisms that result in 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. Click the **Folders** tab.
   The **Folders** panel on the left lists the folders for the filter set selected in the **Folder for Filter Set** list. Fields on the right show the name, color, and description of the selected folder.

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

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

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

4. To add a folder:

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

      The Add Folder dialog box opens.

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

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

   c. Click **OK**.

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

5. In the **Description** box, type a description for the new folder.
6. To change the tab position of the folder on the **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 67 and "Creating a Filter from the Issue Auditing View" on page 68.

Adding a Folder to a Filter Set

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

To add a folder to a filter set:

1. Select **Tools > Project Configuration**.

   The Project Configuration dialog box opens.

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

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

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

   The Add New Folder to Filter Set dialog box opens.

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

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

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

Renaming a Folder

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

To rename a folder:

1. Select **Tools > Project Configuration**.
2. Click the **Folders** tab.
3. In the **Filter Set** list, select **(All Folders)**.
4. Select the folder in the **Folders** list.

   The folder properties are displayed on the right.
5. Type the new name for the folder.

   The folder name changes in the **Folders** list as you type.
6. Click **OK**.

The new folder name displays on the tabs.

Removing a Folder

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

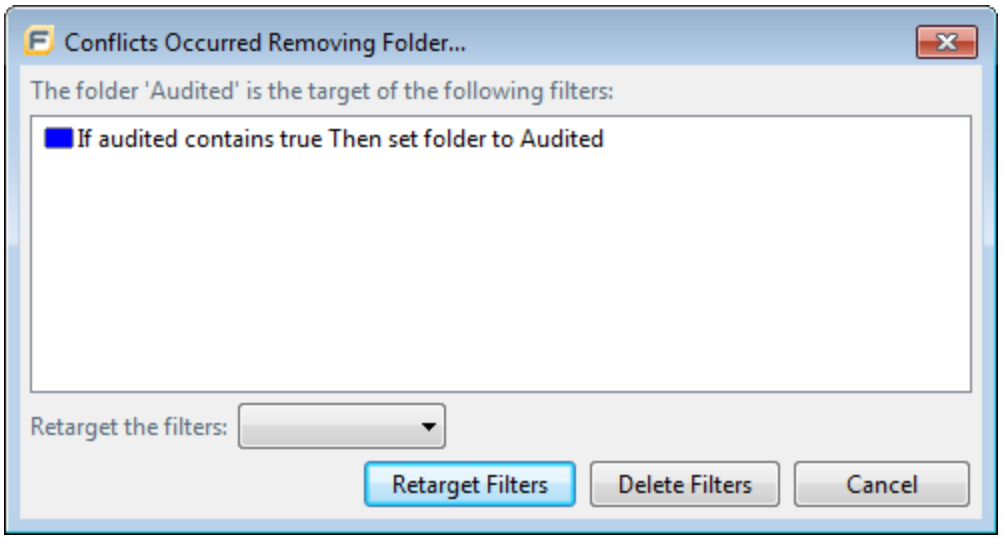
To remove a folder:

1. Select **Tools > Project Configuration**.
2. Click the **Folders** tab.
3. Select a filter set from the **Filter Set** list.

   The **Folders** list displays the folders in the selected filter set.
4. Select the folder, and then next to **Folders**, click **Delete Folder**  .

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

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



Do one of the following:

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

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

The folder is no longer displayed as a tab in the **Issues** view.

Configuring Custom Tags for Auditing

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

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

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

You can also define custom tags from Fortify Software Security Center, either directly with issue template uploads through Fortify Software Security Center, or from Audit Workbench through issue templates in FPR files.

Note: Although you can add new custom tags from 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.

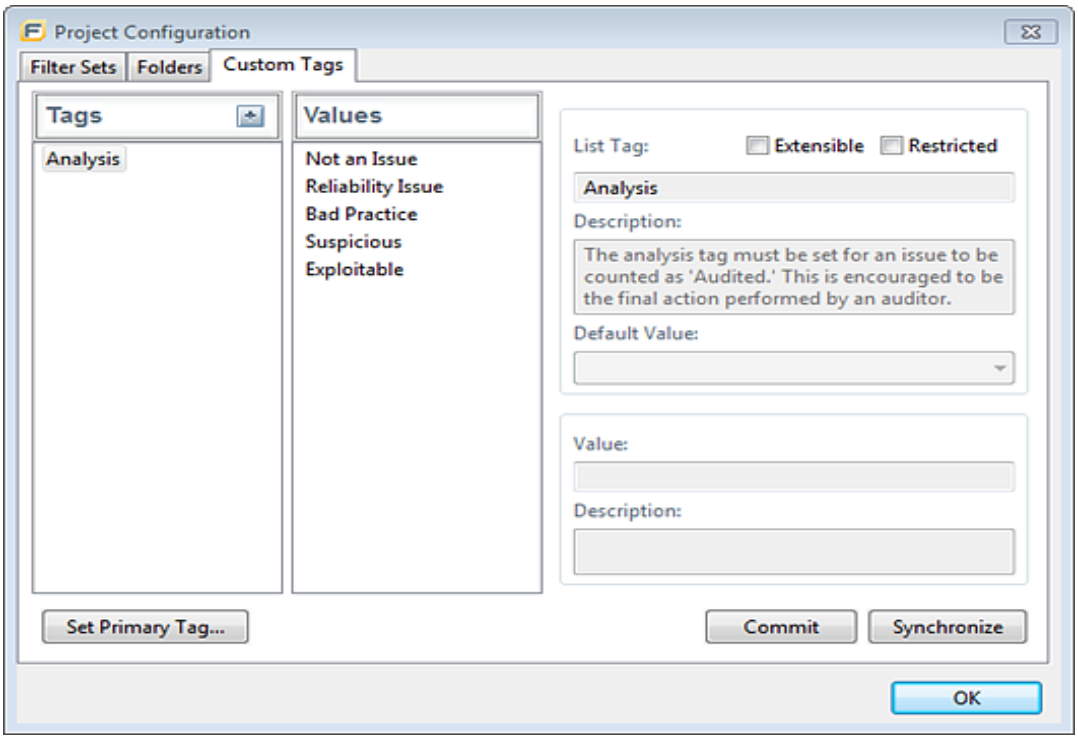
After you define a custom tag, it is displayed below the **Analysis** tag, which enables you to specify values as they relate to specific issues. Custom tags are also available in other areas of the interface, such as in the **Group By** list as a way to group issues in a folder, in the search field 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: If you previously deleted tags, these are listed and you can re-enable them. To create a new tag, click **Create New**.

   The Add New Tag dialog box opens.
4. In the **Name** box, type a name for the new tag.

   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 of 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.
   - Enter 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. Enter a description of the value in the **Description** box.
   e. Repeat steps a through d for each additional value required for the new tag.
9. To make this custom tag the primary tag:

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

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

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

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

Deleting a Custom Tag

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

To delete a custom tag:

1. Select **Tools > Project Configuration**.
   The Project Configuration dialog box opens.
2. Click the **Custom Tags** tab.
3. Select the tag from the **Tags** list.
4. Next to **Tags**, click **Delete Tag**  .
5. Click **OK**.

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

Synchronizing Custom Tags with Fortify Software Security Center

To synchronize custom tags for an audit project that has been uploaded to 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, enter your Fortify Software Security Center credentials.

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

Issue Template Sharing

Once an issue template is associated with an audit project, all changes made to that template, such as the addition of folders, custom tags, filter sets, or filters, apply to the audit project. The issue template is stored in the FPR when the audit project is saved. For information about how to associate the issue template with an audit project, see "Importing an Issue Template" 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. Click the **Filter Sets** tab.
3. Click **Export**.

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

The current template settings are saved to an XML file.

Importing an Issue Template

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

To import an issue template:

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

   The Locate Template File dialog box opens.
4. Select the issue template file to import.
5. Click **Open**.

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

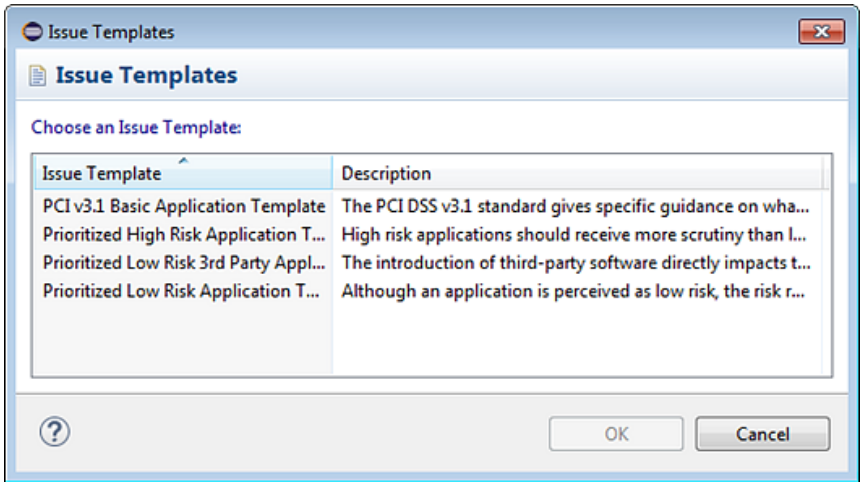
Note: You can also click **Reset to Default** to return the settings to the default issue template.

Synchronizing Filter Sets and Folders

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

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

   A message advises you that downloading filter sets and folders from Fortify Software Security Center overwrites your local filter sets and folders.
4. To proceed with the synchronization, click **Yes**.
5. If required, provide your Fortify Software Security Center credentials, and then click **OK**.
6. If the current issue template does not exist on Fortify Software Security Center, do the following:



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

Audit Workbench downloads the filter sets and folders from the selected issue template on 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 on Fortify Software Security Center, do the following:

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

   The Update Existing Issue Template or Add Issue Template dialog box opens, depending on whether the issue template already exists in Fortify Software Security Center.
6. Do one of the following:
   a. To upload filter sets and folders to the issue template, click **Yes**.
   b. To add the issue template that contains the current set of custom tags to Fortify Software Security Center, click **Yes**.

Advanced Configuration

This section contains the following topics:

Bug-Tracking System Integration

Audit Workbench provides a plugin interface to integrate with bug-tracking systems. This enables you to file bugs directly from Audit Workbench. For a list of supported bug-tracking systems, see the *HPE Security Fortify Software System Requirements* document.

To select the plugin to use:

1. Open an audit project.
2. Select **Tools > Select Bugtracker**.

Example source code for the bug tracking plugins is available in `<sca_install_dir>/Samples/advanced/BugTrackerPlugin<bugtracker>`, where <*bugtracker*> is the name of the bug-tracking system.

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

Important: If your custom bug-tracker accesses supporting JAR files, you must add them to the `Bundle-ClassPath` attribute in your bug-tracker's `MANIFEST.MF` OSGI bundle descriptor file.

Public APIs

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

Penetration Test Schema

HPE Security Fortify also provides a generic penetration test schema (`pentestimport.xsd`) that you can view in `<sca_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 HPE Security Fortify generic format (using XSLT or a similar technology). You can then open or merge these translated results automatically, similar to the built-in parsers. See "Third-Party Penetration Results" on page 92 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 particular context understood best by the development team. No technology can fully determine whether a suspect behavior can be 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.

The topics in this section provide information about how to audit scan results opened in Audit Workbench.

This section contains the following topics:

Working with Audit Projects

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

Opening an Audit Project

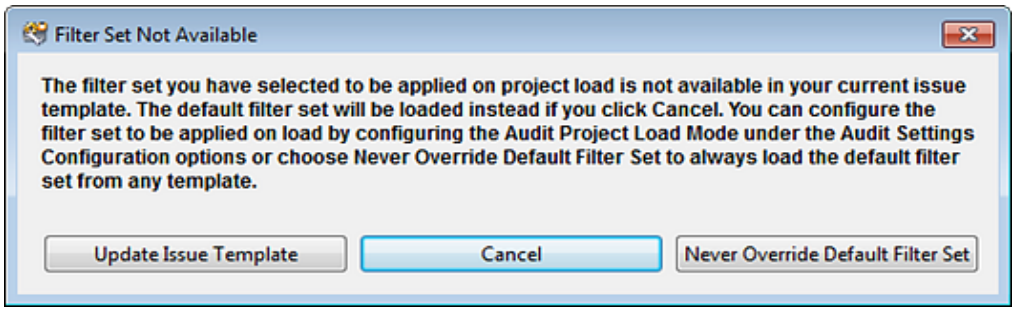
To open an audit project:

1. Start 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 the Fortify on Demand Server.

To resolve this, do one of the following:

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

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

  A warning is displayed to let you know that the update cannot be undone.
- 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 on Fortify Software Security Center collaboratively with other Fortify Software Security Center users.

To start a collaborative audit:

1. Start Audit Workbench.

   If you already have an audit project open, close it.
2. Under **Open Collaborative Audit**, click **Sign In**.
3. Type your Fortify Software Security Center logon credentials.

   Audit Workbench displays a list of applications you have permission to access.
4. Select an application version to audit.

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

   The audit project file is downloaded from Fortify Software Security Center and opened in Audit Workbench.
5. Audit the project as described in "Evaluating Issues" on page 85.
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" on the next page.

Refreshing Permissions From Fortify Software Security Center

The Security Content 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 panel, select **Server Configuration**.
3. Click **Refresh Permissions for the Current Audit**.
4. Click **OK**.

Merging Audit Data

Audit data are 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), 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 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, 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 migrate earlier FPR files to the current format. For more information about how to use this utility, see the *HPE Security Fortify Source Code Analyzer User Guide*.

Migration for Fortify Static Code Analyzer version 5.x projects occurs automatically with the merge action. Merging combines all analysis information resolving conflicts using the values set in the primary project. The merge produces an output project file that contains the analysis information from the primary project.

The signature action prints the full signature information. Exit codes are used to relay the validity of the signature.

Additional Metadata

Each issue in Audit Workbench contains additional metadata that is not produced by HPE's 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 `<sca_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 the project was downloaded 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**.

To upload results to Fortify Software Security Center:

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

   Note: If you see a message that the application version is not committed or does not exist, this

indicates that you opened an audit project that was previously associated with an application version that does not exist on the 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 on Fortify Software Security Center) are uploaded.

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 76 and "Committing Filter Sets and Folders" on page 79 for more information.

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.

   For information about the **Issues** view, see "About Viewing Scan Results" on page 34.
2. In the Issue Auditing view, read the abstract on the **Summary** tab. This abstract provides high-level information about the issue, such as the analyzer that found the issue.

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

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

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

   Note: If you select a different value for **Analysis** than the **AA_Prediction** value set by Audit Assistant, and you select **Include** from the **AA_Training** list, then the next time the data is submitted to Audit Assistant, it updates the information used to predict whether or not an issue represents a true vulnerability. For more information about Audit Assistant, see the *HPE Security 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 to which you want to assign the same analysis value.
2. Press **Ctrl** + **Shift** + **A** (**Cmd** + **Shift** + **A** on Mac OS).

   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 **Summary** tab.

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

Performing Quick Audits for Custom Tags

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

To use a custom tag for quick audits:

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

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

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

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

For information about custom tags, see "Configuring Custom Tags for Auditing" on page 73.

Adding Screen Captures to Issues

You can attach a screen shot or other image to an issue. Attached images are stored in the FPR file and can be accessed 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 panel, click the **Screenshots** tab.
3. Click **Add**.
   The New Screenshot dialog box opens.
4. Browse to and select the image file.
5. (Optional) In the **Description** box, type a description.
6. Click **Add**.

Viewing Images

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

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

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

Creating Issues for Undetected Vulnerabilities

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

To create an issue:

1. Select the object in the line of code in the source code view.
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 **Summary** tab includes `Custom Issue`. You can edit the issue to include audit information, just as you can other issues.

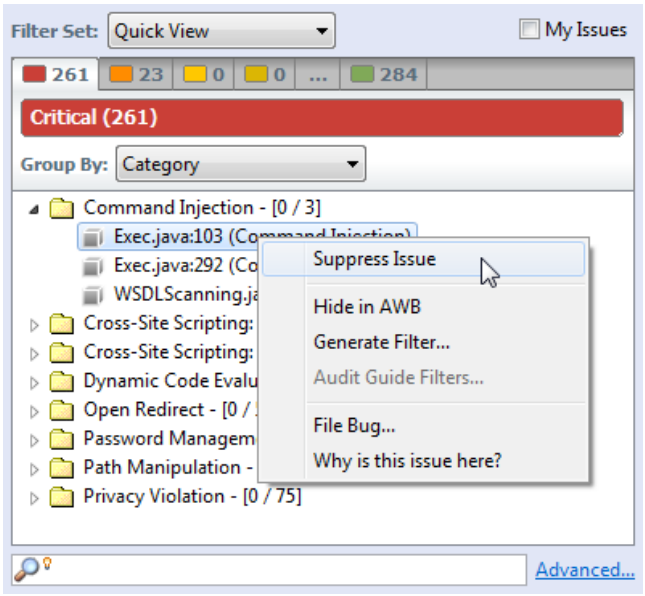
Suppressing Issues

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

To suppress an issue, do one of the following:

- In the **Issues** view, select the issue, and then, on the **Summary** 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.



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 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 **Summary** 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 tracking 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 **Summary** tab, click **File Bug**  .

   When you submit a bug for first time, the Configure Bugtracker Integration dialog box opens. (For information about configuring the plugin with bug tracking systems, see "Bug-Tracking System Integration" on page 79.) Select a bug-tracking application, and then click **Select**

   The File Bug dialog box opens.
2. Specify all required values and review the issue description. Depending on the integration and your bug tracking application, the values include items such as the bug tracking application URL, product name, severity level, summary, and version.
3. Click **Submit**.

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

If you use Fortify Software Security Center, you can submit an issue as a bug using a bug-tracking system configured through Fortify Software Security Center.

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

1. Select the issue in the **Issues** view, and then, on the **Issue Summary** tab, click the **File Bug** icon.

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

If your bug-tracking system requires you to log on, 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 (HPE Security Fortify WebInspect Agent, Fortify Static Code Analyzer, or HPE Security 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 HPE Security 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.

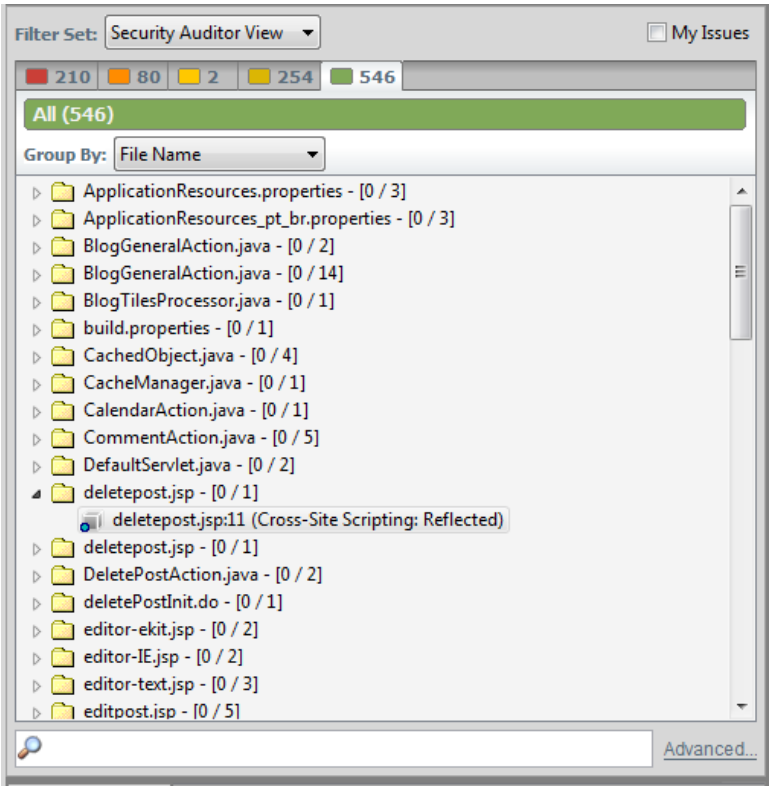
Audit Workbench provides additional information to help you resolve these correlated issues and mitigate the risks they present. In Audit Workbench, this additional information is presented as Correlation Justification.

Using Correlation Justification

To use correlation justification:

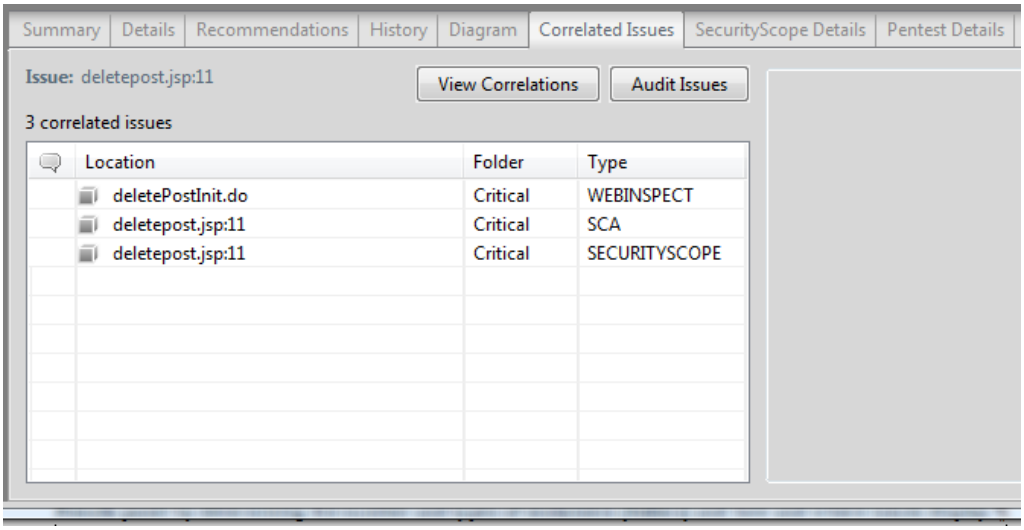
1. In the Issues view, select a correlated issue.

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



2. In the **Issues Auditing** view, click the **Correlated Issues** tab.

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

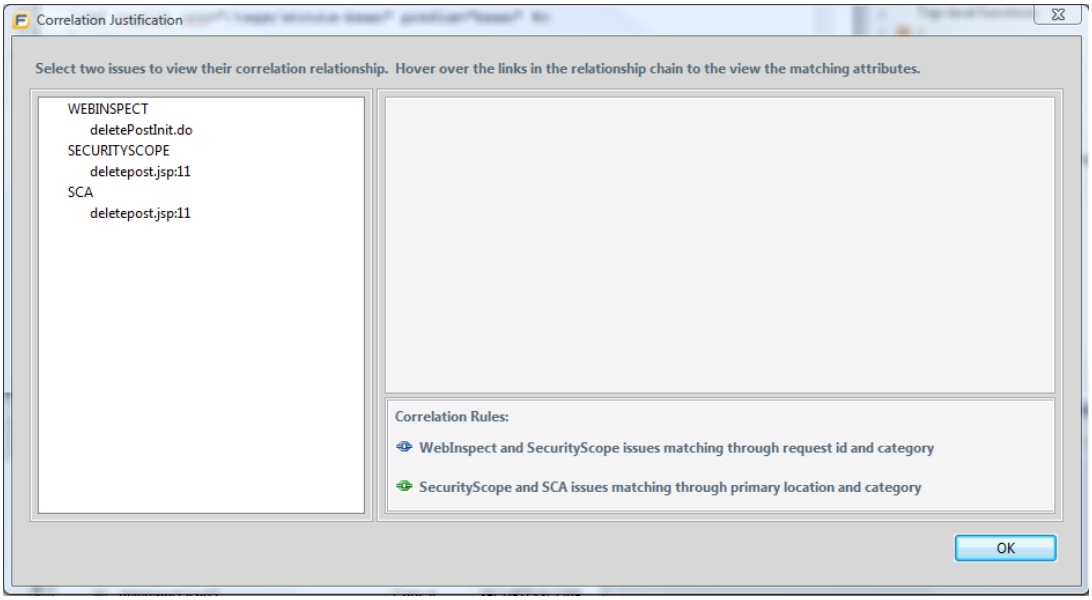


Because you first selected a correlated issue, the **View Correlations** button is available.

3. Click **View Correlations**.

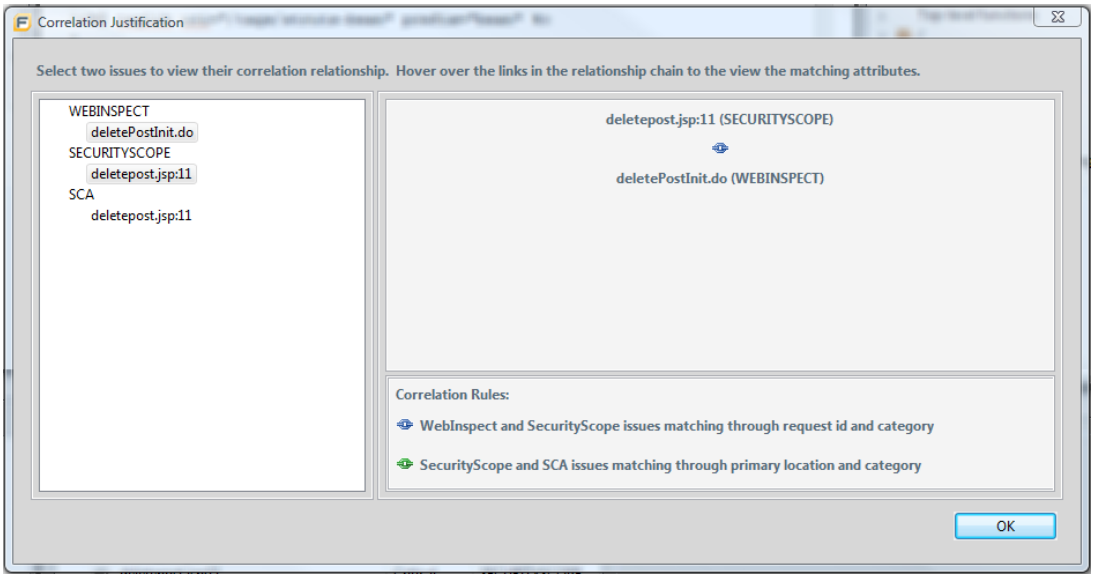
   The Correlation Justification dialog box opens and displays the following three panels:

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

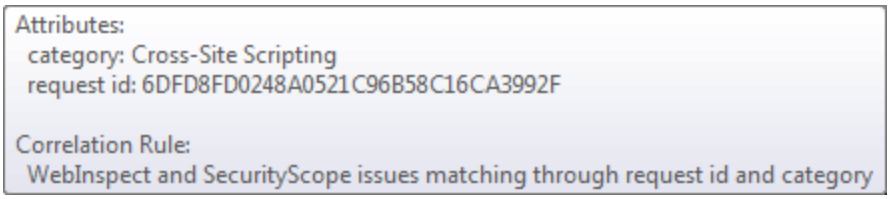


4. To select two issues, press **Ctrl**, and then click each issue.

   The relationship panel 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 panel.



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.

Third-Party Penetration Results

HPE Security Fortify software includes built-in parsers for the following penetration test (pentest) tools and services:

- HPE Security Fortify WebInspect
- IBM AppScan
- Application Security Inc. AppDetective
- White Hat

Each of these tools and services produces results in an XML file format. The built-in parsers take in a pentest results file as input and dynamically create HPE Security Fortify issues.

The parsers are automatically invoked when you open up a pentest results file on its own, or in the context of an FPR file. When you merge a pentest results file into an FPR, the pentest results are persisted in the FPR file during a save.

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, Audit Workbench displays the penetration test details on the **Pentest Details** tab. The following table lists the penetration test details.

Pentest Detail	Description
Path	URL minus the context and parameters.
Referer	Referrer header in the request.
Method	Either GET or POST.
Parameters	Parameters included in the HTTP query.

Pentest Detail	Description
Cookies	Cookies included in the HTTP query.
Attack Type	Type of pentest attack conducted (URL, 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: Audit Workbench Reports

Audit Workbench provides two types of reports:

- 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:

BIRT Reports

The following table describes the BIRT reports available.

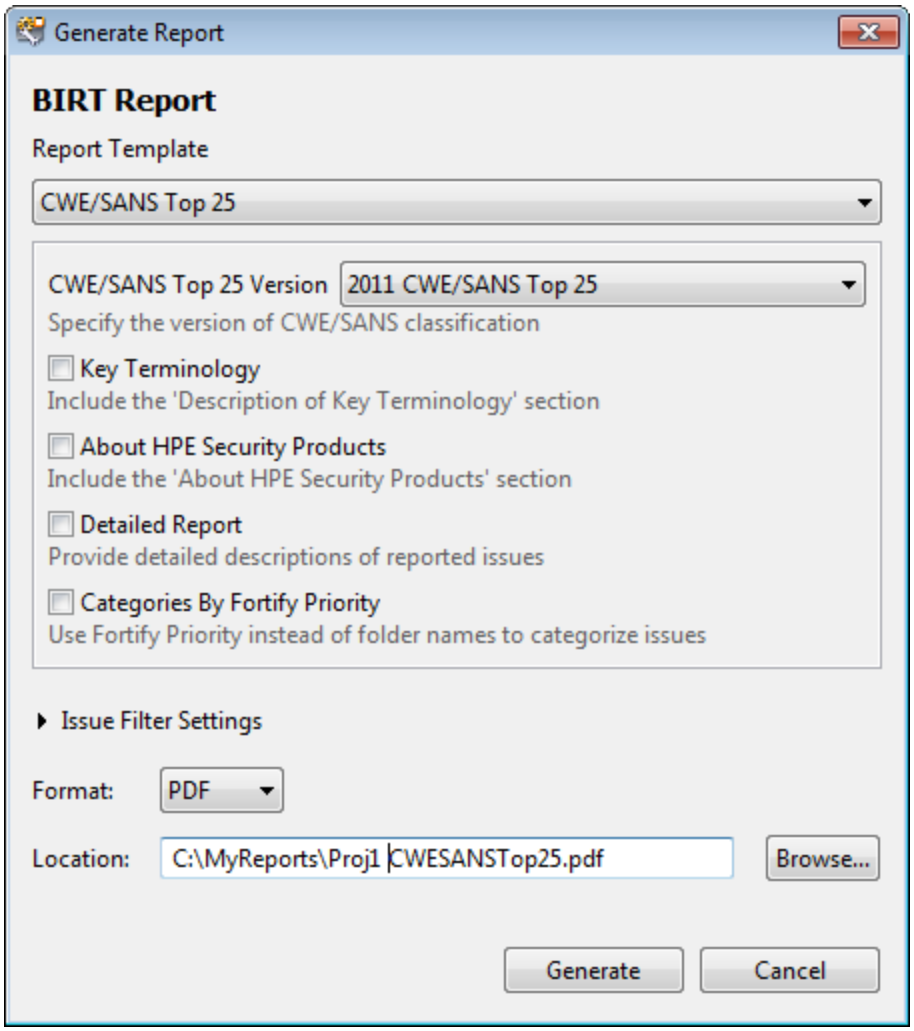
Report Template	Description
CWE/SANS Top 25	This report details findings related to the CWE/SANS Top 25 most dangerous programming errors uncovered and provides information about where and how to address the findings.
Developer Workbook	This report, which is targeted at project managers and developers, contains all of the information needed to understand and fix issues discovered during an audit.
DISA STIG	This report addresses DISA compliance STIG violations It includes information about where and how to fix the issues, and describes the technical risks posed by unremediated violations. The report also includes an estimate of the effort required to fix, verify, and test the findings.
FISMA Compliance: FIPS 200	This report addresses FISMA compliance through FIPS-200 violations detected. It provides information about where and how to fix the issues and describes the technical risks posed by unremediated violations. The report also includes an estimate of the effort required to fix, verify, and test the findings.
OWASP Mobile Top 10	This report details the top ten OWASP mobile-related findings. It provides information on where and how to fix specific issues and describes the technical risk posed by the unremediated findings. The reports also provide estimates of the effort required to fix, verify, and test the findings.
OWASP Top 10	This report details the top ten OWASP-related findings. It provides information about where and how to fix the issues and describes the technical risks posed by unremediated violations. The reports also provides estimates of the effort required to fix, verify, and test the findings.

Report Template	Description
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.”

Generating BIRT Reports

To generate a BIRT report:

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

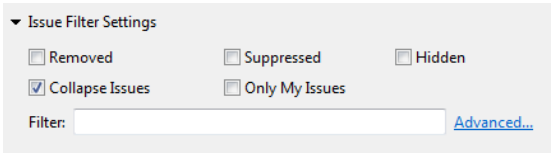


2. From the **Report Template** menu, select the type of report you want.
3. If available for the template, select the template version.

4. Select the information to include in the report.

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

   a. To include Description of Key Terminology in the report, select the **Key Terminology** check box.
   b. To include the About HPE Security Products section in the report, select the **About HPE Security Products** check box.
   c. To include detailed descriptions of reported issues, select the **Detailed Report** check box.
   d. To categorize issues by Fortify Priority instead of folder names, select the **Categories By Fortify Priority** check box.
5. To filter information from the report, click **Issue Filter Settings**.

   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 61.
6. Click the **Format** menu to specify the format for the report (PDF, HTML, DOC, or XLS).

   Note: When you open the XLS file in Excel, you might get a warning that the file format and the file extension do not match. You can safely open the file in Excel.
7. To specify an alternate location to save the report, click **Browse** and 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

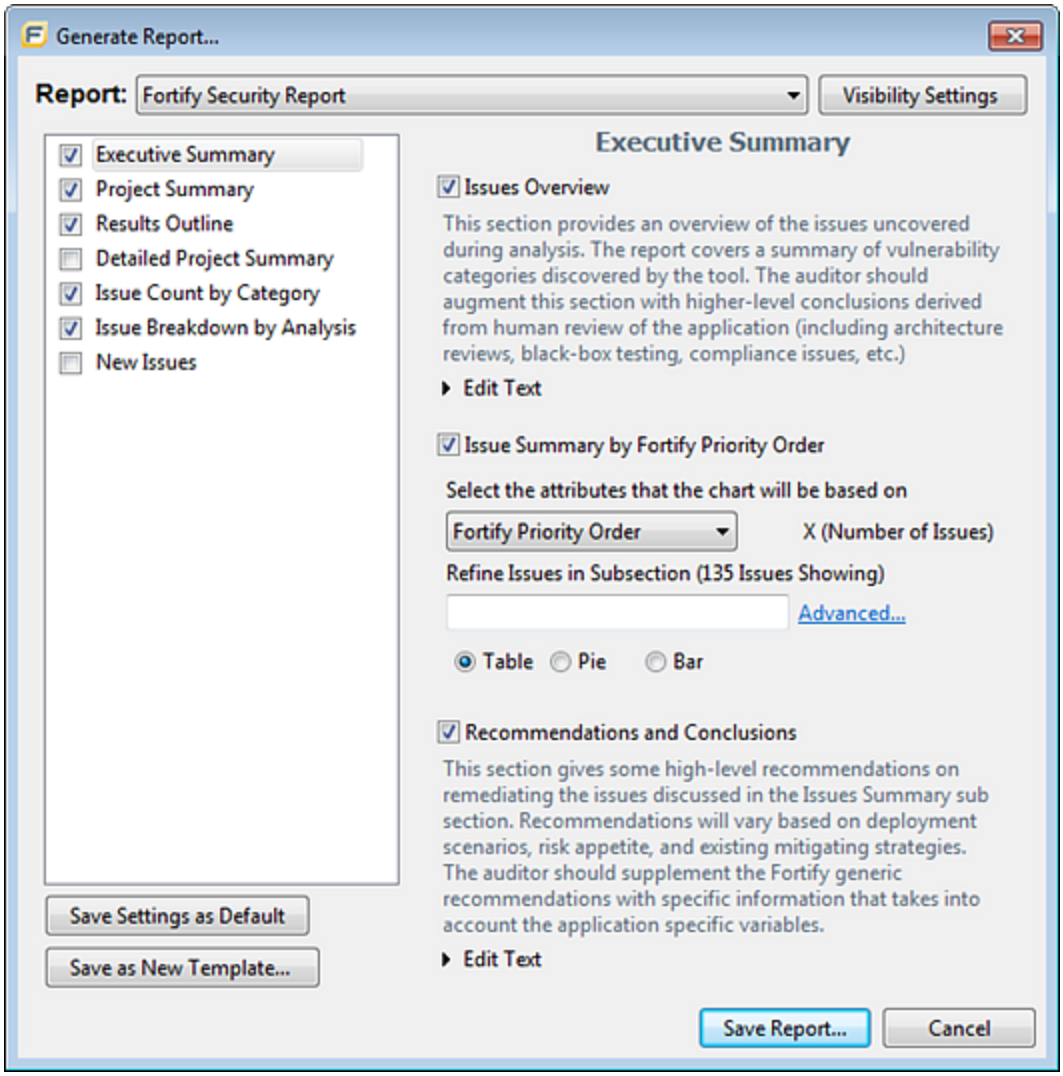
There are several report templates, which you can either modify to suit your needs, or use as they are. Each report template includes several sections and subsections. The subsections provide charting and

other data collection and presentation options. For detailed descriptions of the report templates, see "Legacy Report Components" on page 125.

Opening Legacy Report Templates

To open a report template:

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



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

The Generate Report dialog box displays the report template settings.

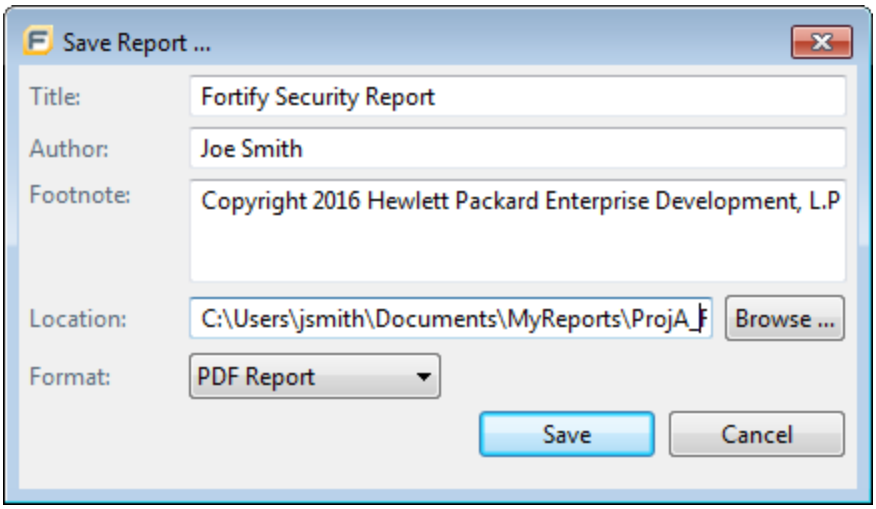
Generating Legacy Reports

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

To run a report:

1. Select **Tools > Generate Legacy Report**.
2. Select a report template from the **Report** list.
3. (Optional) Make changes to the report section settings.
4. Click **Save Report**.

   The Save Report dialog box opens.



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

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

6. Click **Save**.

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

Legacy Report Templates

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

The legacy report templates include:

- **Fortify Developer Workbook**—A comprehensive list of all categories of issues found and multiple examples of each issue. This report also gives a high-level summary of the number of issues in each category.
- **Fortify Scan Summary**—High-level information based on the category of issues that Fortify Static Code Analyzer found as well as a project summary and a detailed project summary.

- **Fortify Security Report**—A mid-level report that provides comprehensive information on the analysis performed and the high-level details of the audit that was performed. It also provides a high-level description and examples of categories that are of the highest priority.
- **OWASP Top Ten *<year>***—High-level summaries of uncovered vulnerabilities organized based on the top ten issues identified by the Open Web Security Project (OWASP).

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 102). The following sections provide information about how to view report templates and customize them to address your reporting needs.

Selecting Report Sections

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

To select sections to include in the report:

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

The section details are displayed to the right of the dialog box. For instructions on how to edit each section, see "Saving Legacy Report Templates" on page 102.

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

Editing Report Subsections

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

Editing Text Subsections

To edit a text subsection:

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

1. Click **Edit Text**.

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

Variable	Description
`$AUDIT_GUIDE_SUMMARY$`	List of filters created by answering Audit Guide questions
`$CLASSPATH_LISTING$`	JAR files used in the scan, one relative path per line

Variable	Description
$COMMANDLINE_ARGS$	Complete list of command-line options (same format as project summary)
$FILE_LISTING$	List of files scanned, each file in format `<relative file path> # Lines # kb <timestamp>`
$FILTERSET_DETAILS$	List of filters in use by current filter set
$FILTERSET_NAME$	Name of current filter set
$FORTIFY_SCA_VERSION$	Fortify Static Code Analyzer version
$LIBDIR_LISTING$	Libdirs specified for the scan, one relative path per line
$TLOC$	Total lines of code
$NUMBER_OF_FILES$	Total number of files scanned
$PROJECT_BUILD_LABEL$	Build label of project
$PROJECT_NAME$	Build ID
$PROPERTIES$	Complete list of properties set for the analysis phase (same format as project summary)
$RESULTS_CERTIFICATION$	Complete certification detail with a list of validity on a per file basis (see 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)
RUN_INFO	Content from the **Project Summary Runtime Analysis** tab
$SCAN_COMPUTER_ID$	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

Variable	Description
$SCAN_USER$	Username for the user who performed the scan
$SOURCE_BASE_PATH$	Source base path of codebase
$TOTAL_FINDINGS$	Number of findings, not including suppressed or removed issues
$WARNINGS$	Complete list of warnings that occurred (same format as the project summary)
$WARNING_SUMMARY$	Number of warnings found in scan

Editing Results List Subsections

To edit a result list subsection:

1. Select the check box next to the subsection title to include this text in the report.

   A description of the results list displays below the subsection title.
2. Click the issues list heading to expand the options.
3. Select the attributes that the results list will be grouped by.

   For the list of attributes to group by, see "Working with Issues" on page 53. If you group by category, the recommendations, abstract, and explanation for the category are also included in the report.
4. You can refine the issues shown in this subsection with the search functions.

   For more details on the search syntax, see "Searching for Issues" on page 60.

   The **Refine Issues in Subsection** field displays the query.
5. Select or clear the **Limit number of Issues in each group** check box.
6. If you selected the check box, type the number of issues to display per group.

Editing Charts Subsections

To edit a chart subsection:

1. Select the check box next to the subsection title to include this text in the report.

   A chart description is displayed below the subsection title.
2. Select the attributes that the chart data will be grouped by.

   For the list of attributes to group by, see "Working with Issues" on page 53.
3. You can refine the issues shown in this subsection by using the search functions.

   For more details on the search syntax, see "Searching for Issues" on page 60.

   The query is displayed in the **Refine Issues in Subsection** field.
4. Select the chart type (table, bar, or pie) to display.

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**.

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

Saving Changes to Report Templates

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

To save changes a report template:

1. Select **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 report template XML files is:

`<sca_install_dir>/Core/config/reports`

You can also customize the logos used in the reports by specifying paths or replacing `header.png` and `footer.png` in this directory.

Adding Report Sections

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

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

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

Adding Text Subsections

In a text subsection, you can include the `Title` tag, the `Description` tag, and the `Text` tag. In the `Text` tag, you can provide the default content, although you can edit the content before you generate a report. For a description of the text variables available to use in text subsections, see "Editing Report Subsections" on page 99. The following XML is the `Overall number of results` subsection in the `Results Outline` section:

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

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

Adding Results List Subsections

In a results list subsection, you can include the `Title` tag, the `Description` tag, and the `IssueListing` tag. In the `IssueListing` tag, you can define the default content for the limit and set `listing` to `true`. You can include the `Refinement` tag either with or without a default statement, although you can edit the content before you generate a report. To generate a results list, the `Chart` tag attribute `chartType` is set to `list`. You can also define the `Axis` tag. The following XML is the `Vulnerabilities Examples by Category` subsection in the `Results Outline` section:

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

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

Adding Charts Subsections

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

The following code shows an example of a charts subsection:

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

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

Chapter 7: Using the Functions View

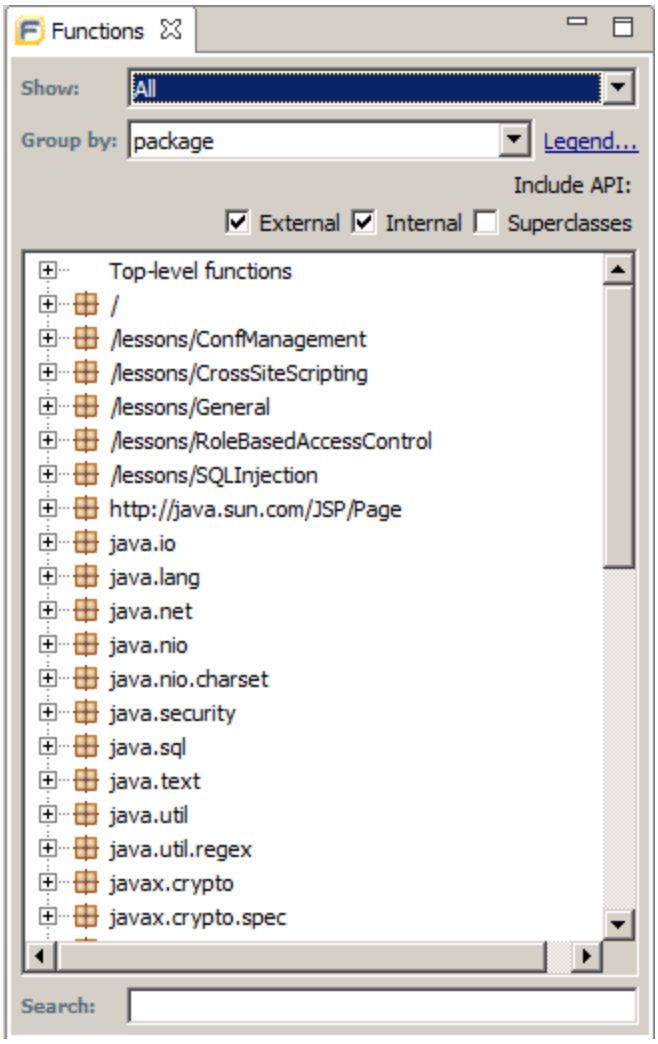
Fortify Static Code Analyzer identifies all functions declared or called in your source code. You can use the **Functions** view in Audit Workbench to determine where a function is located in the source code, whether the function was covered by a security rule, and which rule IDs matched the function. 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

To open the **Functions** view:

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



   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**.

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 are identified as a source of tainted data by the Rulepack used in the most recent scan, 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**.

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 appears in the source code.

To show where a function is located in 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 Evidence View

You can synchronize the **Functions** view with the **Analysis Evidence** view so that, after you select an issue or a trace node from the **Analysis Evidence** 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 Evidence** view:

1. In the Functions view, from the **Group by** list, select **class**.
2. In the top-right corner of the **Analysis Evidence** view, click the **Synchronize with Functions**

View icon.

The **Functions** view displays the class that contains the item you selected in the **Analysis Evidence** 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 on a function and 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 displays 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 "Searching for Issues" on page 60, or create visibility or folder filters.

To display the rule IDs:

1. Open a project in 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 launch the **Custom Rules Wizard** from the **Functions** view.

To write a rule for a function:

1. Open a project in 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. Enter the information as directed by the wizard, and save the new rule to a custom Rulepack.
4. To re-scan the translated files with the custom Rulepack:
   a. Select **Options > Options**.
   b. In the left panel, 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 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 Audit Workbench and how to report issue to HPE Security Fortify Technical Support.

This section contains the following topics:

Creating Archive Logs for HPE Security Fortify Technical Support

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

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

1. In the Audit Workbench menu bar, select **Help > Contact HPE Security Fortify Support**.
2. In the Create HPE Security 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**.

   The Save Successful dialog box opens.
6. To contact HPE Security Fortify Technical Support and supply the archive file, follow the instructions provided in the Save Successful dialog box.
7. Click **OK**.

Using the Debugging Option

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

To enable debugging:

1. Navigate to the `<sca_install_dir>/Core/config` directory and open the `fortify.properties` file.

2. You can either enable debug mode for all Fortify Software Security Center components or for specific components. Remove the comment tag (#) from in front of the property and set the value to `true`.

Property	Description
`com.fortify.Debug`	If set to `true`, all the Fortify Software Security Center components run in debug mode.
`com.fortify.awb.Debug`	If set to `true`, Audit Workbench runs in debug mode.
`com.fortify.eclipse.Debug`	If set to `true`, the Eclipse Complete Plugin runs in debug mode.
`com.fortify.VS.Debug`	If set to `true`, HPE Security Fortify Package for Visual Studio runs in debug mode.

For help diagnosing the problem, send the log files to HPE Security Fortify Technical Support. On Windows systems, log files are located in the following directories:

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

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

- `<userhome>/.fortify/sca<version>/log`
- `<userhome>/.fortify/AWB-<version>/log`
- `<userhome>/.fortify/AWB-<version>/.metadata`

Addressing the org.eclipse.swt.SWTError Error

On Unix systems, 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 Audit Workbench.

Scenario	For more information...
Opening or auditing a large and complex FPR file	"Allocating More Memory for Audit Workbench" on the next page

Scenario	For more information...
Running a scan on a very large and complex project	"Allocating More 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 More Memory for Audit Workbench

To increase the memory allocated for Audit Workbench, set the environment variable `AWB_VM_OPTS`. (For example, set `AWB_VM_OPTS=-Xmx700M` to allocate 700 MB to Audit Workbench.) If you choose to set `AWB_VM_OPTS`, do not allocate more memory than is physically available. Overallocation degrades performance.

If you are using Mac OS, edit the `eclipse.ini` file (`<sca_install_dir>/Auditworkbench.app/contents/MacOS/eclipse.ini`) to change the `-Xmx500m` argument to `-Xmx700m` or higher.

In Audit Workbench, issue information is persisted to disk. This persisted information is reloaded on demand and thereby decreases the required memory footprint of 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 value as follows:

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

Allocating More 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 Audit Workbench. See "Scanning Large and Complex Projects" on page 25.
- Before your start 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 the Amount of Memory Used by External Processes

You can specify how much memory external processes such as the Instance ID Migrator (iidmigrator) use by specifying the `com.fortify.model.ExecMemorySetting` setting in the `fortify.properties` file. The default setting is as follows:

```
com.fortify.model.ExecMemorySetting=600
```

The value for this setting, which is expressed in MB, is used to specify the maximum heap size. In this case, 600 equates to `-Xmx600M`.

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, Audit Workbench displays following warning message:

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

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

To configure how Audit Workbench handles this issue for future occurrences:

1. Select **Options > Options**.
2. In the left panel, select **Audit Configuration**.
3. 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**
4. Click **OK**.

Resetting the Default Views

If you have closed or moved views, such as the **Issues** view or the **Summary** 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 panel, click **Audit Configuration**.
3. On the **Appearance** tab, click **Reset Interface**.

Appendix A: Sample Files

Your Fortify SCA and Applications installation includes a number of sample files that you can use when testing or learning to use Fortify Static Code Analyzer. The sample files are located in the following directory:

`<sca_install_dir>/Samples`

The `Samples` directory contains two subdirectories: `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 Audit Workbench.

The `basic` subdirectory includes an assortment of simple language-specific samples. The `advanced` subdirectory contains more advanced code samples and samples that enable you to integrate Fortify Static Code Analyzer with your bug tracking and build systems.

This section contains the following topics:

Basic Samples

The following table describes the sample files in the `<sca_install_dir>/Samples/basic` directory and provides a list of the vulnerabilities that the samples demonstrate. Many of the samples includes a `README.txt` file that provides details and instructions on its use.

Folder Name	Description	Vulnerabilities
cpp	A C++ sample file and instructions to analyze code that has a simple dataflow vulnerability. It requires a gcc or cl compiler.	Command Injection Memory Leak
database	A `database.pks` sample file. This SQL sample includes issues in SQL code.	Access Control: Database
eightball	A Java application (`EightBall.java`) that exhibits bad error handling. It requires an integer as an argument. If you supply a file name instead of an integer, it displays the file contents.	Path Manipulation Unreleased Resource: Streams J2EE Bad Practices: Leftover Debug Code

Folder Name	Description	Vulnerabilities
formatstring	The `formatstring.c` file. It requires a gcc or cl compiler.	Format String
javascript	The `sample.js` JavaScript file.	Cross Site Scripting (XSS) Open Redirect
nullpointer	The `NullPointerSample.java` file.	Null Dereference
php	Two PHP files: `sink.php` and `source.php`. Analyzing `source.php` reveals simple dataflow vulnerabilities and a dangerous function.	Cross Site Scripting SQL Injection
sampleOutput	A sample output file (`WebGoat5.0.fpr`) from the WebGoat project located in the `Samples/advanced/webgoat` directory.	
stackbuffer	The `stackbuffer.c` file. It requires a gcc or cl compiler.	Buffer Overflow
toctou	The `toctou.c` file.	Time-of-Check/Time-of-Use (Race Condition)
vb6	The `command-injection.bas` file.	Command Injection SQL Injection
vbscript	The `source.asp` and `sink.asp` files.	SQL Injection

Advanced Samples

The following table describes the sample files in the `<sca_install_dir>/Samples/advanced` directory. Many of the samples include a `README.txt` file that provides further details and instructions on its use.

Folder Name	Description
BugTrackerPlugin<*bugtracker*>	Includes source code for the supported bug tracking plugin.
c++	A sample solution for different supported versions of Visual Studio. To use this sample, you must have the following installed: • A supported version of Visual Studio Visual C/C++ • Fortify Static Code Analyzer and the package for your Visual Studio version

Folder Name	Description
	The code includes a Command Injection issue and an Unchecked Return Value issue.
configuration	A sample Java EE application that has vulnerabilities in its web module deployment descriptor `web.xml`.
crosstier	A sample that has vulnerabilities that span multiple application technologies (Java, PL/SQL, JSP, struts). The output contains several issues of different types, including two Access Control vulnerabilities. One of these is a cross-tier result. It has a dataflow trace from user input in Java code that can affect a `SELECT` statement in PL/SQL.
csharp	A simple C# program that has SQL Injection vulnerabilities. Versions are included for different supported versions of Visual Studio. After successful completion of the scan, you should see the SQL Injection vulnerabilities and one Unreleased Resource vulnerability. Other categories might also be present, depending on the Rulepacks used in the scan.
customrules	Several simple source code samples and Rulepack files that illustrate how four different analyzers: Semantic, Dataflow, Control Flow, and Configuration interpret rules. This folder also includes several miscellaneous samples of real-world rules that you can use to scan real applications.
ejb	A sample Java EE cross-tier application with Servlets and EJBs.
filters	A sample that uses the Fortify Software Security Center `-filter` option.
findbugs	A sample that demonstrates how to run the FindBugs static analysis tool (http://findbugs.sourceforge.net) together with Fortify Static Code Analyzer and filter out results that overlap.
java1.5	A sample Java file: `ResourceInjection.java`. The result file should include a Path Manipulation and a J2EE Bad Practices vulnerability.
javaAnnotations	A sample application that illustrates problems that might arise from its use and how to fix the problems using the Fortify Java Annotations. This example illustrates how the use of Fortify Annotations can result in increased accuracy in the reported vulnerabilities. The accompanying `Java Annotations Sample.txt` file describes the potential problems and solutions associated with vulnerability results.
JavaDoc	JavaDoc directory for the `public-api` and `WSClient`.
riches.java	A Java EE 1.4 sample web application with various known security vulnerabilities including Cross-Site Scripting, SQL Injection, and Command Injection.

Folder Name	Description
riches.net	A .NET 4.0 sample web application with various known security vulnerabilities including Cross-Site Scripting, SQL Injection, and Command Injection.
webgoat	The WebGoat test Java EE web application provided by the Open Web Application Security Project (https://www.owasp.org). This directory contains the WebGoat 5.0 source code.

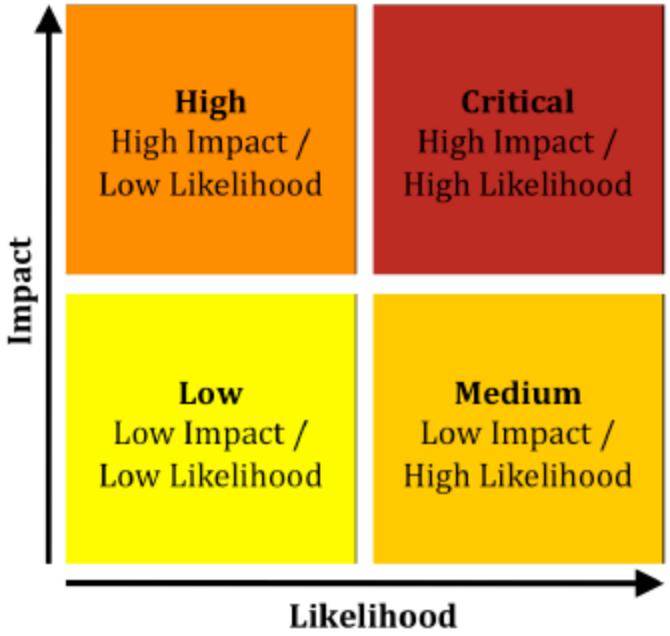
Appendix B: Static Analysis Results Prioritization

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

This section contains the following topics:

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 as a whole 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 particular vulnerability, Fortify Static Code Analyzer takes a probabilistic approach to prioritizing vulnerabilities. Risk is defined quantitatively, as follows:

```
risk = impact x 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 particular 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 can be exploited. 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 particular user session to a member variable of a singleton object in a web application. Since, under the singleton model, the same class instance is used to service all requests, 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 fairly simple to exploit after it is found, finding race conditions can be difficult 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

HPE Security 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:

```
likelihood = accuracy x confidence x 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 · 5 · 3)/25 = 3 (High) Risk = Critical Estimated remediation effort = 5
Cross-Site Request Forgery	2	1	5	2	Impact = 2 (Low) Likelihood = (1 · 5 · 2)/25 =

Category	Impact	Accuracy	Confidence	Probability	Risk
					<1 (Low) Risk = Low Estimated remediation effort = 12
Cross-Site Scripting: Reflected	5	5	5	5	Impact = 5 (High) Likelihood = (5 · 5 · 5)/25 = 5 (High) Risk = Critical Estimated remediation effort = 1
Cross-Site Scripting: Persistent	5	5	1	5	Impact = 5 (High) Likelihood = (5 · 1 · 5)/25 = 1 (Low) Risk = Medium Estimated remediation effort= 1

Appendix C: 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

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
Executive Summary 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.	**Issues Overview** Editable overview of the issues, including the date of the scan, number of issues, name of the project, scan summary and total number of findings.
	Issue Summary by Fortify Priority Order 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: • Critical - High impact and high likelihood. Critical issues are easy for the attacker to discover and exploit to result in extensive asset damage. • High - High impact but low likelihood. High priority issues are often difficult to discover and exploit, but can result in extensive asset damage.

Section	Subsection
	• 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. You can present this information in a table or in a pie or bar chart.
	Recommendations and Conclusions High-level recommendation on remediating the issues listed in the Issues Summary subsection. You can edit the text in this subsection.
Project Summary Provides project summary information such as the codebase, scan information, results certifications, and so on.	**Code-Base Summary** Summary of the analyzed codebase. You can edit the text element of this subsection.
	Scan Information Analysis details. You can edit the text element of this subsection.
	Results Certification Results certifications summary. You can edit the text element of this subsection.
	Attack Surface Attack surface summary. You can edit the text element of this subsection.
	Filter Set Summary Summary of the filter set used in the report. You can edit the text element of this subsection.
	Audit Guide Summary Summary of the audit guide. You can edit the text element of this subsection.
Results Outline	**Overall Number of Results**

Section	Subsection
Provides an outline of the results that Fortify Static Code Analyzer produced during the scan.	Total number of results that Fortify Static Code Analyzer produced during the scan. You can edit the text element of this subsection.
	Vulnerability Examples by Category Results summary of highest-level issues by category.
Detailed Project Summary Provides a detailed project summary.	**Files Scanned** List of all scanned files. You can edit the text element of this subsection.
	Reference Elements List of all libraries that Fortify Static Code Analyzer used during the translation phase of analysis. You can edit the text element of this subsection.
	Rulepacks List of Rulepacks that Fortify Static Code Analyzer used in the analysis. You can edit the text element of this subsection.
	Properties List of properties that Fortify Static Code Analyzer set during the analysis phase. You can edit the text element of this subsection.
	Commandline Arguments List of all options that Fortify Static Code Analyzer uses during the translation phase of analysis. You can edit the text element of this subsection.
	Warnings List of all warnings issued during both translation and analysis phases of the scan. You can edit the text element of this subsection.
Issue Count by Category Provides a chart of Issues by category. This chart is	**Issues By Category** Chart of issues by category. You can

Section	Subsection
configurable.	present the information in a table or as a pie or bar chart.
Issue Breakdown by Analysis Provides a chart of issues by analysis. This chart is configurable.	**Issue By Analysis** Chart of issues by analysis. You can present the information in a table or as a pie or bar chart.
New Issues Provides a chart of all new issues. This chart is configurable.	**New Issue** Chart of new issues. You can present the information in a table or as a pie or bar chart.

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
Report Overview Provides a high-level overview of report findings.	**Report Summary** Editable overview of vulnerability. This includes the date of the scan, the project name, and the total number of vulnerabilities.
	Issue Summary by Fortify Priority Order Issues charted based on Fortify Priority Order. You can present the information in a table or as a pie or bar chart.
Issue Summary Provides the number and categories of vulnerabilities.	**Overall number of results** Total number of vulnerabilities. You can edit the text element of this subsection.
	Issues by category Chart of issues based on category. You can present the information in a table or as a pie or bar chart.
Results Outline Provides an outline of the results that Fortify Static Code Analyzer produced during the scan.	**Vulnerability Examples by Category** Results summary of highest-level issues by category.

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
Report Overview Provides a high-level overview of report findings.	**Report Summary** Editable overview of vulnerabilities, including the date of the scan, the project name, and the total number of vulnerabilities.
	Issue Summary Chart of issues grouped by a selected attribute such as category, kingdom, or analysis type. You can present the information in a table or as a pie chart or bar chart.
Issue Breakdown by OWASP Top Ten Provides a chart of issues organized by OWASP top ten security risks.	**Issue Breakdown by OWASP Top Ten** Chart of issues grouped by a selected attribute such as category, kingdom, or analysis type. You can present the information in a table or as a pie chart or bar chart.
Results Outline Provides an outline of the results that Fortify Static Code Analyzer produced during the scan.	**Vulnerability Examples by OWASP Top Ten** Lists the vulnerabilities organized by the OWASP top ten. You can use select listing to further refine and organize the vulnerabilities that Audit Workbench provides in the report.

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
Issue Count by Category Provides a chart of issues by category.	**Issues By Category** Chart of issues grouped by a selected attribute such as category, kingdom, or analysis type. You can present the information in a table or as a pie chart or bar chart.
Project Summary	**Code Base Summary** Summary of the codebase that Fortify Static Code Analyzer

Section	Subsection
Provides project summary information, including codebase summary and general scan information.	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.
	Scan Information 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.
	Results Certification Results certifications information, including the results certification summary and the details of the results certification. You can edit the text element of this subsection.
Detailed Project Summary Provides detailed project summary information including the files scanned, reference elements, and so on.	**Files Scanned** Lists all files Fortify Static Code Analyzer scanned. You can edit the text element of this subsection.
	Reference Elements List of libraries that Fortify Static Code Analyzer used during the translation phase. You can edit the text element of this subsection.
	Rulepacks List of Rulepacks that Fortify Static Code Analyzer used during the analysis. You can edit the text element of this subsection.
	Properties Lists the properties that Fortify Static Code Analyzer set during the analysis. You can edit the text element of this subsection.
	Commandline Arguments Lists the arguments that the program passed to Fortify Static Code Analyzer during analysis. You can edit the text element of this subsection.
	Warnings Lists the warnings that occurred during analysis. You can edit the text element of this subsection.

Send Documentation Feedback

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

Feedback on User Guide (HPE Security Fortify Audit Workbench 17.10)

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 HPFortifyTechPubs@hpe.com.

We appreciate your feedback!