
Micro Focus Fortify Extension for Visual Studio

Software Version: 19.1.0

User Guide

Document Release Date: May 2019

Software Release Date: May 2019



Legal Notices

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

<https://www.microfocus.com>

Warranty

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

Restricted Rights Legend

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

Copyright Notice

© Copyright 2009 - 2019 Micro Focus or one of its affiliates

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

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

Contents

Preface	6
Contacting Micro Focus Fortify Customer Support	6
For More Information	6
About the Documentation Set	6
Change Log	7
Chapter 1: Introduction	8
Fortify Extension for Visual Studio	8
Fortify Security Content	9
Installation	9
Upgrades	9
Related Documents	10
All Products	10
Micro Focus Fortify Software Security Center	11
Micro Focus Fortify Static Code Analyzer	11
Chapter 2: Using the Fortify Extension for Visual Studio	12
Configuring Scan Settings	12
Using Quick Scan Mode	13
Configuring Advanced Scan Options	14
Scanning Solutions	14
Synchronizing with Fortify Software Security Center	15
About Viewing Scan Results	16
Analysis Results Window	17
Filter Sets	17
Folders (Tabs)	18
Group By List	18
Customizing the Issues Display	18
Viewing Project Summary Information	18
Analysis Evidence Window	20

Issue Auditing Window	21
Code Editor	26
Grouping Issues	27
Creating a Custom Group By Option	28
Searching for Issues	29
Search Modifiers	30
Search Query Examples	34
Performing Simple Searches	35
Performing Advanced Searches	35
Using the Audit Guide to Filter Issues	36
Auditing Scan Results	36
Auditing Issues	37
Suppressing Issues	37
Viewing Suppressed Issues	38
Submitting an Issue as a Bug	38
About Issue Templates	38
Saving Issue Templates	39
Exporting Issue Templates	39
Importing Issue Templates	40
Configuring Custom Tags for Auditing	40
Creating a Custom Tag	40
Deleting a Custom Tag	41
Creating a Filter Set	42
Creating a Filter from the Analysis Results Window	42
Creating a Filter from the Filters Tab	43
Copying a Filter to Another Filter Set	44
Managing Folders	44
Creating a Folder	44
Adding a Folder to a Filter Set	45
Renaming a Folder	46
Removing a Folder	46
Scan Results Reports	47
About BIRT Reports	47
Generating BIRT Reports	48
About Legacy Reports	50
Running Legacy Reports	50
Opening Legacy Report Templates	50

Legacy Report Templates	51
Working with Audit Projects	57
Opening Audit Projects	57
About Merging Audit Data	58
Merging Audit Data	58
Performing a Collaborative Audit	58
Uploading Results to Fortify Software Security Center	60
About Updating Security Content	60
Configuring Security Content Updates	61
Updating Security Content	61
Scheduling Automatic Security Content Updates	61
Manually Updating Security Content	62
Importing Custom Rules	62
Integrating with a Bug Tracker Application	62
Filing Bugs to Team Foundation Server	62
Using the Debug Option	63
Chapter 3: Remediating Results from Fortify Software Security Center	64
Connecting to Fortify Software Security Center	64
Working with Applications	64
Connecting to a Fortify Software Security Center Application	65
Viewing and Selecting Issues in an Application	65
Working with Issues	67
Issue Details Tab	67
Recommendation Tab	69
Description Tab	69
History Tab	70
Customizing Issue Visibility	70
Searching for Issues	70
Assigning Users to Issues	70
Assigning Tags to Issues	71
Locating Issues in Source Code	71
Send Documentation Feedback	72

Preface

Contacting Micro Focus Fortify Customer Support

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

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

<https://softwaresupport.softwaregrp.com>

To Call Support

1.844.260.7219

For More Information

For more information about Fortify software products:

<https://software.microfocus.com/solutions/application-security>

About the Documentation Set

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

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

Change Log

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

Software Release / Document Version	Changes
19.1.0	Updated: Minor edits
18.20	Updated: Minor edits
18.10	Updated: <ul style="list-style-type: none"><li data-bbox="542 800 1105 831">• Minor edits to incorporate branding changes<li data-bbox="542 852 1370 926">• "About Updating Security Content" on page 60 - Clarified how you import security content manually and how to import custom rules

Chapter 1: Introduction

This guide describes how to use the Fortify Extension for Visual Studio to scan and analyze your project source code to uncover security vulnerabilities (issues), which you can then evaluate and remediate.

This section contains the following topics:

- [Fortify Extension for Visual Studio](#) 8
- [Fortify Security Content](#) 9
- [Installation](#) 9
- [Upgrades](#) 9
- [Related Documents](#)10

Fortify Extension for Visual Studio

The Fortify Extension for Visual Studio works with the Visual Studio integrated development environment (IDE). The extension integrates into the Visual Studio IDE as a software extension.

Software security analysis typically consists of the following phases:

- Analysis—Scan a codebase for vulnerabilities
- Auditing—Review the analysis results to eliminate false positives and prioritize remediation efforts
- Remediation—Fix and eliminate security vulnerabilities in your code

The Fortify Extension for Visual Studio uses Micro Focus Fortify Static Code Analyzer and Fortify Secure Coding Rulepacks to locate security vulnerabilities in your solutions and projects (includes support for the following languages: C/C++, C#, VB.NET, and ASP.NET). The scan results are displayed in Visual Studio and includes a list of issues uncovered, descriptions of the type of vulnerability each issue represents, and suggestions on how to fix them.

Your organization can also use the Fortify Extension for Visual Studio with Micro Focus Fortify Software Security Center to manage applications and assign specific issues to developers.

You can connect with Fortify Software Security Center to review the reported vulnerabilities and implement appropriate solutions from Visual Studio.

Fortify Security Content

Micro Focus Fortify Static Code Analyzer uses a knowledge base of rules to enforce secure coding standards applicable to the codebase for static analysis. Fortify Security Content (security content) consists of Fortify Secure Coding Rulepacks and external metadata:

- Secure Coding Rulepacks describe general secure coding idioms for popular languages and public APIs
- External metadata includes mappings from the Fortify categories to alternative categories (such as CWE, OWASP Top 10, and PCI DSS)

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

Installation

You install the Fortify Extension for Visual Studio by selecting the extension during the Micro Focus Fortify Static Code Analyzer and Applications installation (which includes Audit Workbench and other plugins that you can install). For installation instructions, see the *Micro Focus Fortify Static Code Analyzer User Guide*.

During the Fortify Static Code Analyzer installation, make sure that you select the extension that corresponds to the Visual Studio version installed on your system.

If you plan to scan your code from Visual Studio, make sure that you select the **Update security content after installation?** check box at the end of the installation unless your administrator has set up an alternative way to deliver Fortify Security Content to you.

Upgrades

After you install the Fortify Extension for Visual Studio, when you subsequently upgrade Micro Focus Fortify Static Code Analyzer and select to also install the Fortify Extension for Visual Studio, the new version of the extension is automatically upgraded. You can upgrade Fortify Static Code Analyzer (along with Audit Workbench and any plugins you have installed) manually or automatically from Audit Workbench. For instructions, see the *Micro Focus Fortify Audit Workbench User Guide*.

Related Documents

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

Note: You can find the Micro Focus Fortify Product Documentation at <https://www.microfocus.com/support-and-services/documentation>. Apart from the Release Notes, all guides are available in both PDF and HTML formats.

All Products

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

Document / File Name	Description
<i>About Micro Focus Fortify Product Software Documentation</i> About_Fortify_Docs_<version>.pdf	This paper provides information about how to access Micro Focus Fortify product documentation. Note: This document is included only with the product download.
<i>Micro Focus Fortify Software System Requirements</i> Fortify_Sys_Reqs_<version>.pdf	This document provides the details about the environments and products supported for this version of Fortify Software.
<i>Micro Focus Fortify Software Release Notes</i> FortifySW_RN_<version>.txt	This document provides an overview of the changes made to Fortify Software for this release and important information not included elsewhere in the product documentation.
<i>What's New in Micro Focus Fortify Software <version></i> Fortify_Whats_New_<version>.pdf	This document describes the new features in Fortify Software products.
<i>Micro Focus Fortify Open Source and Third-Party License Agreements</i> Fortify_OpenSrc_<version>.pdf	This document provides open source and third-party software license agreements for software components used in Fortify Software.

Micro Focus Fortify Software Security Center

The following documents provide information about Fortify Software Security Center. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website at

<https://www.microfocus.com/documentation/fortify-software-security-center>.

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

Micro Focus Fortify Static Code Analyzer

The following documents provide information about Fortify Static Code Analyzer. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website at

<https://www.microfocus.com/documentation/fortify-static-code>.

Document / File Name	Description
<i>Micro Focus Fortify Static Code Analyzer User Guide</i> SCA_Guide_<version>.pdf	<p>This document describes how to install and use Fortify Static Code Analyzer to scan code on many of the major programming platforms. It is intended for people responsible for security audits and secure coding.</p>
<i>Micro Focus Fortify Static Code Analyzer Custom Rules Guide</i> SCA_Cust_Rules_Guide_<version>.zip	<p>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.</p> <p>Note: This document is included only with the product download.</p>

Chapter 2: Using the Fortify Extension for Visual Studio

Use the Fortify Extension for Visual Studio to perform Micro Focus Fortify Static Code Analyzer scans, review and audit analysis results, and remediate issues in Visual Studio.

This section contains the following topics:

Configuring Scan Settings	12
Scanning Solutions	14
Synchronizing with Fortify Software Security Center	15
About Viewing Scan Results	16
Auditing Scan Results	36
About Issue Templates	38
Configuring Custom Tags for Auditing	40
Creating a Filter Set	42
Managing Folders	44
Scan Results Reports	47
Working with Audit Projects	57
About Updating Security Content	60
Integrating with a Bug Tracker Application	62
Using the Debug Option	63

Configuring Scan Settings

The analysis configuration settings enable you to configure security content and the amount of memory Micro Focus Fortify Static Code Analyzer uses during the scan.

To configure the analysis settings:

1. Open a solution in Visual Studio.
2. Select **Fortify > Options**.
3. In the Options dialog box, select **Project Settings** on the left.

The Project Settings dialog box opens to show the **Analysis Configuration** tab.

4. To specify the scope of the settings, do one of the following:
 - To customize the settings for the projects in the open solution only, select the **Enable Project Specific Settings** check box.
 - To change the default scan settings for all projects scanned from this Visual Studio instance, click **Configure Defaults**.
5. By default, Fortify Static Code Analyzer treats SQL files as **T-SQL**. If your files use PL/SQL, from the **SQL Type** list, select **PL/SQL**.

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

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

Note: Do not allocate more than two thirds of the available physical memory.
7. To customize the security content that you want to use, clear the **Use all installed security content** check box, and then select the Secure Coding Rulepacks and any custom Rulepacks that you want to use.
8. Click **OK**.

Using Quick Scan Mode

Quick Scan mode provides a way to quickly scan your projects for major issues. However, although the scan in Quick Scan mode is significantly faster, it does not provide a robust result set.

When you enable Quick Scan mode, Micro Focus Fortify Static Code Analyzer scans your project using the `fortify-sca-quickscan.properties` file, rather than the standard `fortify-sca.properties` file. By default, this scan searches for high-confidence, high-severity issues. You can edit the `fortify-sca-quickscan.properties` file to specify other properties to use. This file is located in `<sca_install_dir>\Core\config` directory.

To perform a quick scan:

1. With a solution open in Visual Studio, select **Fortify > Options**.
2. Select **Fortify > Options**.
3. In the Options dialog box, select **Project Settings** on the left.
4. Do one of the following:
 - To configure quick scans for the projects in the open solution, select the **Enable Project Specific Settings** check box.
 - To configure quick scans for by default for all projects scanned from this Visual Studio instance, select the **Configure Defaults** link.
5. On the **Advanced Scan Options** tab, select the **Enable quick scan mode** check box.

Configuring Advanced Scan Options

You can specify advanced Micro Focus Fortify Static Code Analyzer scan and translation options. For information about the available options and the proper syntax, see the *Micro Focus Fortify Static Code Analyzer User Guide*.

To change the advanced scan options:

1. With a solution open in Visual Studio, select **Fortify > Options**.
2. In the Options dialog box, select **Project Settings** on the left.
3. To specify the scope of the settings, do one of the following:
 - To customize the settings for the projects in the open solution only, select **Enable Project Specific Settings**.
 - To change the default scan settings for all projects scanned from this Visual Studio instance, click **Configure Defaults**.
4. Click the **Advanced Scan Options** tab.
5. Select **Use additional SCA arguments** and type command-line options for either the translation or scan phase.
6. Click **OK** to save the advanced scan settings.

Scanning Solutions

You analyze the source code from Visual Studio at the solution or project level. A security analysis (scan) performs the following tasks:

- Cleans up old intermediate files used for source code analysis
- Translates all .NET files and other existing supported files, such as T-SQL, in the solution into intermediate files
- Performs the security analysis
- Displays the results

Fortify strongly recommends that you periodically update the security content, which contains Fortify Secure Coding Rulepacks and external metadata. For information about how to update the security content, see ["About Updating Security Content" on page 60](#).

To scan a solution:

1. With a solution open in Visual Studio, select **Fortify > Options**.
2. Verify the Visual Studio configuration as follows:
 - Set the configuration to **debug**.
 - For Visual C++ solutions, verify that all of the project files (*.vcxproj) are modifiable.

3. Start the scan in one of the following ways:
 - To scan at the solution level, select **Fortify > Analyze Solution**.

Note: When you scan your code at the solution level, all projects in the solution are included in the scan including any unloaded projects. To avoid scanning unloaded projects in your solution, you must scan the projects at the project level.

- To scan at the project level, select a project, and then select **Fortify > Analyze Project**.

Note: The **Analyze Project** command is not available for web site projects. To analyze a web site project, choose **Analyze Solution**.

After the scan has finished, the Fortify Extension for Visual Studio displays the results in the auditing interface.

4. Audit the results.
For information, see ["Auditing Issues" on page 37](#).

If the codebase was audited before, results from the previous audit are automatically integrated with the new analysis results.

Note: Micro Focus Fortify Static Code Analyzer invokes scans with the Java Virtual Machine server.

Synchronizing with Fortify Software Security Center

The Fortify Extension for Visual Studio supports the ability to synchronize the local version of your project with the corresponding application version on the Micro Focus Fortify Software Security Center server. With synchronization to the server enabled, each time you load, merge, scan, or save your project locally on your system, the extension automatically uploads your changes to the version of your project on the server. This automatic synchronization prevents work loss during a power outage and enables you to work locally and synchronize your work when you connect at a later time.

Note: The Fortify Extension for Visual Studio supports synchronization between your local project and the corresponding application version on the server.

To enable synchronization to the server:

1. Perform one of the following tasks on your project: scan, partial scan, save, or merge.
A dialog box prompts you to specify whether you want to auto-synchronize your project with the server after a load, merge, save, or scan.
2. Click **OK**.

To change whether synchronization occurs automatically with the server:

1. Select **Fortify > Options**.
2. In the Options dialog box, select **Project Settings** on the left.
3. Click the **Synchronization Options** tab.
4. Either clear the **Auto Synchronize all Projects with Server Application** check box to disable automatic synchronization or select it to enable automatic synchronization.

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

To customize which actions trigger synchronization with the server:

1. Select **Fortify > Options**.
The Options dialog box opens.
2. In the Options dialog box, select **Project Settings** on the left.
3. Select the **Synchronization Options** tab.
4. Select any action to exclude from automatic synchronization, and then click **OK**.

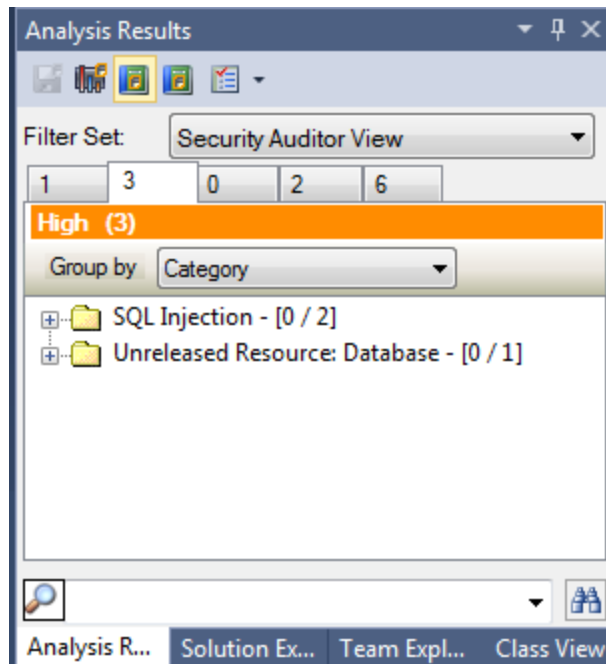
About Viewing Scan Results

After a scan is completed (or after you open an existing audit project), summary results are displayed in the Analysis Results window and in the Project Summary window. The Analysis Evidence and Issue Auditing windows are open, but do not contain any information until you select an issue from the Analysis Results window.

Window	For More Information
Analysis Results	"Analysis Results Window" on the next page
Project Summary	"Viewing Project Summary Information" on page 18
Analysis Evidence	"Analysis Evidence Window" on page 20
Issue Auditing	"Issue Auditing Window" on page 21

Analysis Results Window

The Analysis Results window enables you to group, filter, and select the issues you want to audit.



Filter Sets

The selected filter set controls which issues the Analysis Results window displays. The filter set determines the number and types of containers (folders) and how and where issues are displayed.

Each project can have unique sets because the filter sets are saved in an audit project results file.

The filter sets sort the issues into **Critical**, **High**, **Medium**, and **Low** folders, based on potential severity. All default filter sets have the same sorting mechanism.

The Fortify Extension for Visual Studio provides the following filter sets:

- **Quick View**—This is the default 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 serious issues.
- **Security Auditor View**— This view reveals a broad set of security issues. The Security Auditor View filter contains no visibility filters, and therefore all issues are shown.


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 results open with the **Quick View** filter set selected.

For information about how to create your own filter sets, see ["Creating a Filter Set" on page 42](#).

Folders (Tabs)

The tabs on the Analysis Results window 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 audit projects. For information about how to create your own folders, see ["Creating a Folder" on page 44](#).

Each folder contains a list of issues. An issue is sorted into a folder if its attributes match the folder filter conditions. One folder in each filter set is the default folder, indicated by (default) in the folder name. If an issue does not match any of the folder filters, the issue is listed in the default folder.


Note: To show or hide suppressed, hidden, and removed issues, use the **Visibility** menu . For more information, see ["Customizing the Issues Display" below](#).

Group By List

The **Group By** option sorts the issue list into subfolders. The selected option is applied to all visible folders. Use the **<none>** option to list all issues in the folder without any groups. The **Group By** settings are for the application instance. You can apply the **Group By** option to any audit project opened with that instance of the application.

You can customize the existing groups by changing which attributes the groups are sorted by, adding or removing the attributes to create sub-groupings, and adding your own group options.

Customizing the Issues Display

You can customize the issues displayed in the Analysis Results window. Determine which issues it displays by using the **Visibility** menu  in the Analysis Results toolbar.

The visibility options are as follows:

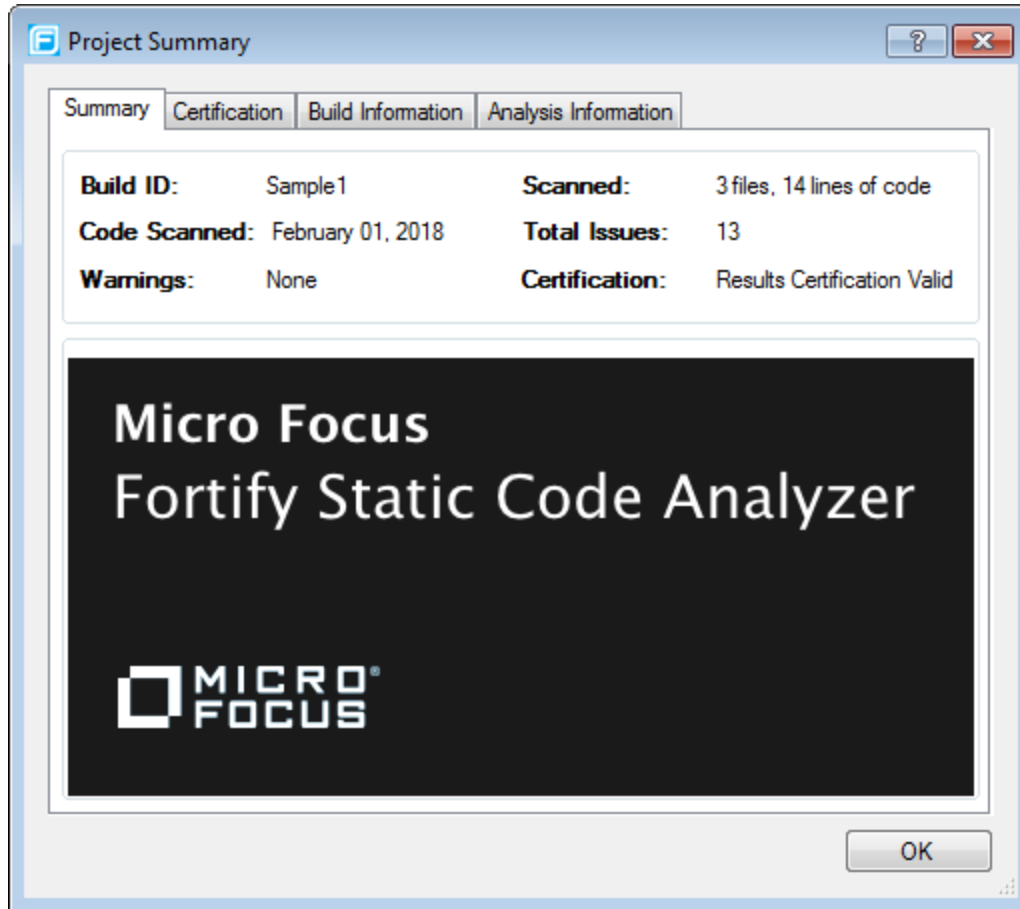
- **Show Removed Issues:** Shows all of the issues you have removed. If you have merged audit data into your current audit project, shows all of the issues that were removed since the previous analysis.
- **Show Suppressed Issues:** Shows all of the issues that you have suppressed.
- **Show Hidden Issues:** Shows all of the issues that have been hidden.
- **Show My Issues:** Shows only your issues.
- **Use Short File Names:** References the issues in the **Issues** view by file name only, instead of by relative path. This option is enabled by default.

Viewing Project Summary Information

The Project Summary window provides detailed information about the scan.

To open the Project Summary dialog box:

1. Open an audit project file (FPR, FVDL, or XML).
2. Select **Fortify > Project Summary**.



The following table describes the information provided on the Project Summary tabs.

Tab	Description
Summary	Displays high level audit project information.
Certification	Displays the result certification status. Results certification is a check to make sure that the analysis has not been altered since Fortify Static Code Analyzer produced it.
Build Information	Displays the following scan information: <ul style="list-style-type: none"> • Build details such as the build ID, number of files scanned, lines of code, and the date of the scan, which might be different than the date the files were translated • List of files scanned with file sizes and timestamps • Libraries referenced for the scan
Analysis Information	Displays the Fortify Static Code Analyzer version, computer details, and the name of the user who performed the scan. The Analysis Information subtabs








Tab	Description
	contain the following information: <ul style="list-style-type: none"> • Security Content—Lists information about the Rulepacks (including the Rulepack name, version, ID, and SKU) and the external metadata used in the scan • Properties—Displays the Micro Focus Fortify Static Code Analyzer properties files settings • Commandline Arguments—Displays the command-line options used to scan the project • Warnings—Lists all errors and warnings that occurred during the analysis. To view more information about an item, click it.














Analysis Evidence Window

When you select an issue, the Analysis Evidence window displays the trace that the analyzer used to produce the issue. This trace is presented in sequential order. For dataflow issues, this trace 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 data flow, the Analysis Evidence window shows the direction of the data flow in this section of the source code.

The Analysis Evidence window uses the icons described in the following table to show how the data flow 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 (HTML form, URL, and so on)
	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

Icon	Description
	An alias is created for a memory location
	Data is read from a variable
	Data is read from a global variable
	Tainted data is returned from a function
	A pointer is created
	A pointer is dereferenced
	The scope of a variable ends
	The execution jumps
	A branch is taken in the codes execution
	A branch is not taken in the codes execution
	Generic
	A runtime source, sink, or validation step
	Taint change

The Analysis Evidence window can contain inductions. Inductions provide supporting evidence for their parent nodes. Inductions consist of:

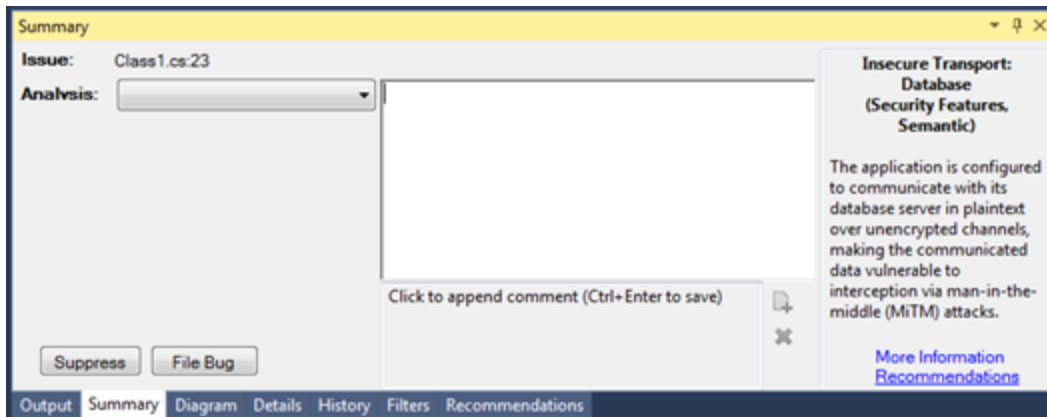
- A text node, displayed in italics as a child of the trace node. This text node is expanded by default.
- An induction trace, displayed as a child of the text node.

To display the induction reference information for that induction, click it.

Issue Auditing Window

The Issue Auditing window displays detailed information about each issue on the following tabs:

- The **Summary** tab displays the following information about the selected issue. Security auditors can add comments and custom tag values to issues from this tab.



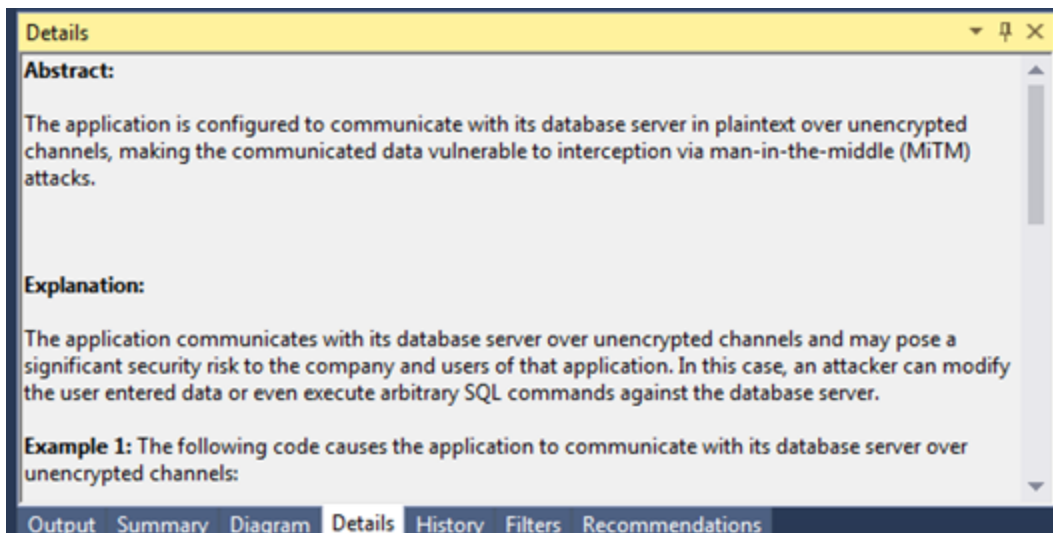
The following table describes the elements of the **Summary** tab.

Element	Description
Issue	Displays the issue location, which includes the file name and line number.
Analysis	Lists values that the auditor can use to assess the issue. Valid values for the Analysis tag are Not an Issue, Reliability Issue, Bad Practice, Suspicious, and Exploitable.
<custom_tagname>	<p>Displays any custom tags if defined for the audit project.</p> <p>If the audit results have been submitted to Audit Assistant in Micro Focus Fortify Software Security Center, then in addition to any other custom tags, the tab displays the following tags:</p> <ul style="list-style-type: none"> • AA_Prediction—Exploitability level that 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. <p>For more information about Audit Assistant, see the <i>Micro Focus Fortify Software Security Center User Guide</i>.</p>
Suppress	Suppresses the issue.
File Bug	Provides access to a supported bug tracking system, such as Bugzilla or Team Foundation Server.

Element	Description
	See the <i>Micro Focus Fortify Software System Requirements</i> document for a list of supported bug tracking systems.
Comments	Appends additional information about the issue as a comment.
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.

For information about auditing, see "[Auditing Issues](#)" on page 37.

- The **Details** tab provides a detailed description of the selected issue and offers guidelines to address it.



Each description includes some or all of the sections described in the following table.

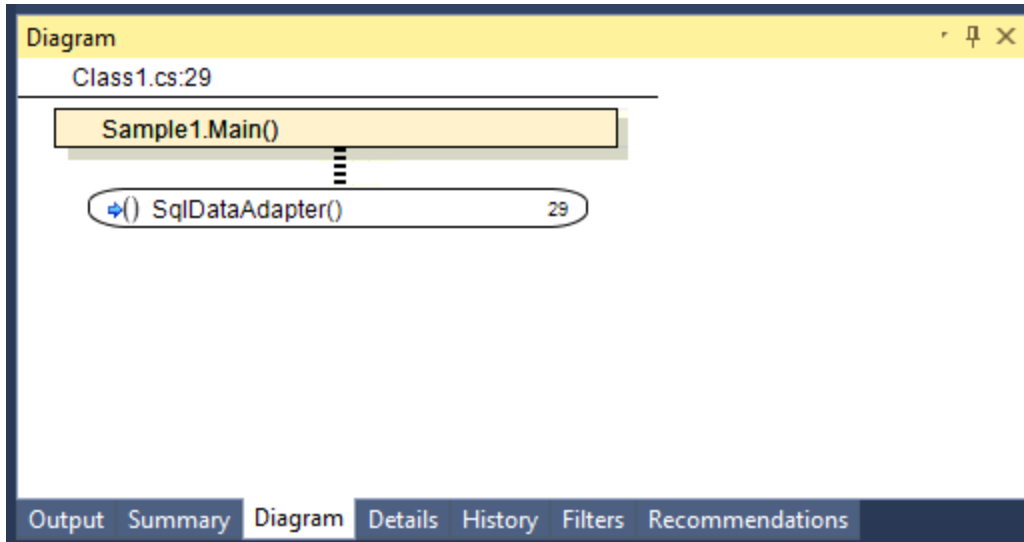
Element	Description
Abstract/Custom Abstract	Provides a summary of the issue, including custom abstracts defined by your organization.

Element	Description
Explanation/Custom Explanation	Provides a description of the conditions in which this type of issue occurs. This description includes a discussion of the vulnerability, the constructs typically associated with it, how it can be exploited, and the potential ramifications of an attack. This element also provides custom explanations defined by your organization.
Instance ID	Provides a unique identifier for the issue.
Primary Rule ID	Identifies the primary rule that found the issue.
Priority Metadata Values	Includes IMPACT and LIKELIHOOD values.
Legacy Priority Metadata Values	Includes SEVERITY and CONFIDENCE values.

- The **Recommendations** tab provides suggestions and examples of how to secure the vulnerability or remedy the bad practice. The recommendations include some or all of the sections described in the following table.

Element	Description
Recommendations/Custom Recommendations	Provides recommendations for how to resolve this type of issue, including examples, and any custom recommendations defined by your organization.
Tips/Custom Tips	Provides tips for this type of issue, including any custom tips defined by your organization.
References/Custom References	Provides reference information, including any custom reference defined by your organization.

- The **History** tab shows a complete list of audit actions, including details such as the date and time, and the name of the user who modified the issue.
- The **Diagram** tab presents a graphical representation of the node execution order, call depth, and expression type of the selected issue. The tab displays information relevant to the rule type. The vertical axis shows the execution order.

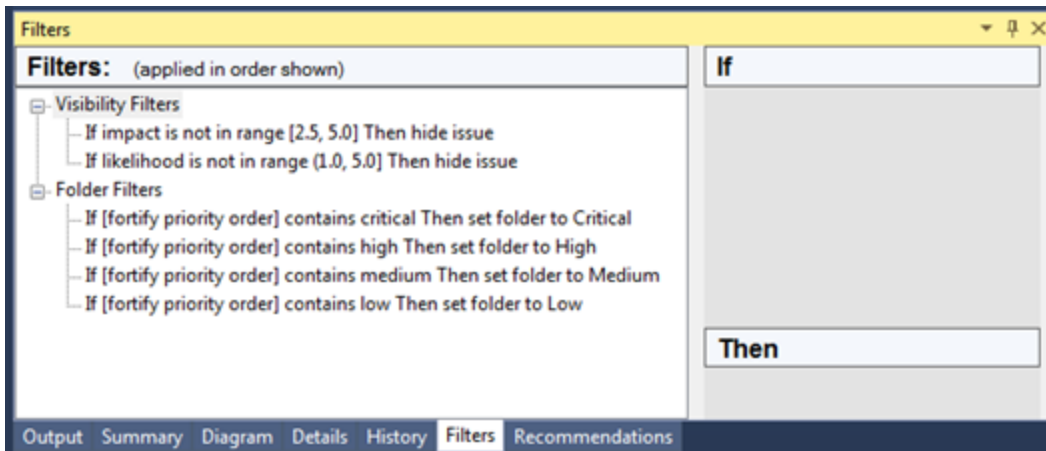


For dataflow issues, the trace starts with the first function to call the taint source, then traces the calls to the source (blue node), and ends the trace at the sink (red node). In the diagram, the source (src) and sink nodes are also labeled. A red X on a vertical axis indicates that the function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

The horizontal axis shows the call depth. A line shows the direction that control is passed. If control passes with tainted data traveling through a variable the line is red, and when it is 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 window. To see the icons and the descriptions, see ["Analysis Evidence Window" on page 20](#).

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



The following table describes the elements of the **Filters** tab.

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

For more information about creating filters, see ["Creating a Filter from the Filters Tab" on page 43](#).

Code Editor

The Code Editor shows the section of code related to the issue selected in the Analysis Results window. When multiple nodes represent an issue in the Analysis Evidence window, the Code Editor shows the code associated with the selected node.

Grouping Issues

The items visible in the navigation tree vary according to which grouping option is selected in the Analysis Results window. 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 using 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 might switch frequently between various groupings. The following table lists descriptions of the standard Group By options.

Option	Description
Analysis	Groups issues by the audit analysis, such as Suspicious, Exploitable, and Not an Issue.
Analysis Type	Groups issues by analyzer product, such as SCA, WEBINSPECT, and SECURITYSCOPE (WebInspect Agent).
Analyzer	Groups issues by analyzer group, such as Control Flow, Data Flow, Semantic, and Structural.
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 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 Micro Focus Fortify Static Code Analyzer impact and likelihood.
Kingdom	Groups issues by the Seven Pernicious Kingdoms classification.
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.
<i><metadata_listname></i>	Groups issues using the alternative metadata external list names (for example, OWASP Top 10 <i><year></i> , CWE, PCI <i><version></i> , STIG <i><version></i> , and so on).

Option	Description
Package	Groups issues by package or namespace. Does not appear for projects for which this option is not applicable, such as C projects.
Priority by Category	A custom group that groups issues by Fortify Priority Order and then by category.
Sink	Groups issues that share the same data flow sink functions.
Source	Groups issues that share the same data flow source functions.
Taint Flag	Groups issues by the taint flags that they contain.
<none>	Displays a flat view without grouping.
<Edit>	Use to create a custom grouping option. Note: This option is not available when you remediate an audit project on Micro Focus Fortify Software Security Center.

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 options.

To create a new Group By option:

1. From the **Group by** list, select **<Edit>**.
The Edit Custom Groupings dialog box opens.
2. To create a grouping from a provided set of group types, select a grouping type from the **Grouping Types** list.

For example, selecting **Category Analyzer** group type 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]
```

3. To create a custom group by option, select **Create New** from the **Grouping Types** list, and then do the following:
 - a. In the Create New dialog box, type a group name, and then click **OK**.
 - b. From the list on the left, select a grouping type, and then click the right arrow to move the option to the **Grouping Order** column.
 - c. Repeat step b to select additional grouping types.

Searching for Issues

You can use the search box located below the issue tree to find specific issues and to limit the issues displayed in a folder. After you type a search term, the label next to the folder name changes to indicate the number of issues that match the search as a subset of the total.

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

Comparison	Description
contains	Searches for a term without any qualifying delimiters
equals	Searches for an exact match if 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.+?/ Note: This search comparison is not available when you remediate audit results stored on Micro Focus Fortify Software Security Center.
number range	Searches for a range of numbers using the standard mathematical interval notation of parentheses and/or brackets to indicate whether the endpoints are excluded or included respectively. Example: (2,4] indicates greater than two and less than or equal to four
not equals	Excludes issues specified by the string by preceding the string with an 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.

Search Modifiers

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

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

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

- To apply the search to all modifiers, type a string, such as `control flow`. This searches all of the modifiers and returns any results that contain the string “control flow”.
- To apply the search to a specific modifier, type the modifier name and the string as follows: `analyzer:control flow`. This returns all results with the analyzer “control flow”.

The following table lists descriptions of the search modifiers. A few modifiers have a shortened modifier name indicated in parentheses in the Modifier column. You can use either modifier name.

Modifier	Description
accuracy	Searches for issues based on the accuracy value specified (0.1 through 5.0).
analysis	Searches for issues that have the specified audit analysis value such as <code>exploitable</code> , <code>not an issue</code> , and so on.
[analysis type]	Searches for issues by analyzer product such as SCA and WEBINSPECT.
analyzer	Searches the issues for the specified analyzer such as <code>control flow</code> , <code>data flow</code> , <code>structural</code> , and so on.
[app defender protected] (def)	Searches for issues based on whether or not Application Defender can protect the vulnerability category (<code>protected</code> or <code>not protected</code>).
audience	Searches for issues based on intended audience such as <code>dev</code> , <code>targeted</code> , <code>medium</code> , <code>broad</code> , and so on.
audited	Searches the issues to find <code>true</code> if the primary custom tag is set and <code>false</code> if the primary custom tag is not set. The default primary tag is the Analysis tag.

Modifier	Description
category (cat)	Searches for the given category or category substring.
class	Searches for issues based on the specified class name.
comments (comment, com)	Searches the comments 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. Micro Focus 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.
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]	<p>Searches for issues that have a priority level that matches the specified priority determined by the Fortify analyzers. Valid values are <i>critical</i>, <i>high</i>, <i>medium</i>, and <i>low</i>, based on the expected <i>impact</i> and <i>likelihood</i> of exploitation.</p> <p>The impact value indicates the potential damage that might result if an issue is successfully exploited. The likelihood value is a combination of confidence, accuracy of the rule, and probability that an attacker can exploit the issue.</p>
historyuser	Searches for issues that have audit data modified by the specified user.
impact	Searches for issues based on the impact value specified (0.1 through 5.0).
[instance id]	Searches for an issue based on the specified instance ID.
[issue age]	Searches for the issue age, which is <i>new</i> , <i>updated</i> , <i>reintroduced</i> , or <i>removed</i> .
[issue state]	Searches for audited issues based on whether or not the issue is an open issue or not an issue (determined by the level of analysis

Modifier	Description
	set for the primary tag).
kingdom	Searches for all issues in the specified kingdom.
likelihood	Searches for issues based on the specified likelihood value (0.1 through 5.0).
line	Searches for issues on the primary location line number. For dataflow issues, the value is the sink line number. Also see "sourceline" on the next page .
maxconf	Searches for all issues that have a confidence value up to and including the number specified as the search term.
minconf	Searches for all issues that have a confidence greater than or equal to the specified value.
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" on the next page and "[source context]" on the next page .
primary	Searches for issues that have the specified primary tag value. By default, the primary tag is the Analysis tag.
primaryrule (rule)	Searches for all issues related to the specified sink rule.
probability	Searches for issues based on the probability value specified (1.0 through 5.0).
[remediation effort]	Searches for issues based on the remediation effort value specified. The valid values are whole numbers from 1.0 to 12.0.
ruleid	<p>Searches for all issues reported by the specified rule IDs used to generate the issue source, sink and all passthroughs.</p> <p>Note: This search modifier is not available when you remediate audit results that are stored on Micro Focus Fortify Software Security Center.</p>

Modifier	Description
severity (sev)	Searches for issues based on the specified severity value (legacy metadata).
sink	Searches for issues that have the specified sink function name. Also see " [primary context] " on the previous page.
source	Searches for dataflow issues that have the specified source function name. Also see " [source context] " below.
[source context]	Searches for dataflow issues that have the source function call contained in the specified code context. Also see " source " above and " [primary context] " on the previous page.
sourcefile	Searches for data flow issues with the source function call that the specified file contains. Also see " file " on page 31
sourceline	Searches for dataflow issues having taint source entering the flow on the specified line. Also see " line " on the previous page.
status	Searches issues that have the status reviewed, unreviewed, 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. Note: This search modifier is not available when you remediate audit results that are stored on Fortify Software Security Center.

Modifier	Description
tracenode	<p>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.</p> <p>Note: This search modifier is not available when you remediate audit results that are stored on Fortify Software Security Center.</p>
tracenodeallpaths	<p>Searches for the specified value in all the steps of analysis evidence.</p> <p>Note: This search modifier is not available in the remediation plugin.</p>
url	Searches for issues based on the specified URL.
user	Searches for issues assigned to the specified user.
<custom_tagname>	<p>Searches the specified custom tag.</p> <p>You can search a list-type custom tag using a range of values. The values of a list-type custom tag are an enumerated list where the first value is 0, the second is 1, and so on. You can use the search syntax for a range of numbers to search for ranges of list-type custom tag values. For example, <code>analysis:[0,2]</code> returns the issues that have the values of the first three analysis values, 0, 1, and 2 (Not an Issue, Reliability Issue, and Bad Practice).</p> <p>To search a date-type custom tag, specify the date in the format: <code>yyyy-mm-dd</code>.</p>
<metadata_listname>	Searches the specified metadata external list. Metadata external lists include <code>[owasp top ten <year>]</code> , <code>[sans top 25 <year>]</code> , <code>[pci <version>]</code> , and others.

Search Query Examples

Consider the following search query examples:

- To search for all privacy violations in file names that contain `jsp` with `getSSN()` as a source, type the following:
`category:"privacy violation" source:getssn file:jsp`

- To search for all file names that contain `com/fortify/awb`, type the following:
`file:com/fortify/awb`
- To search for all paths that contain traces with `mydbcode.sqlcleanse` as part of the name, type the following:
`trace:mydbcode.sqlcleanse`
- To search for all paths that contain traces with `cleanse` as part of the name, type the following:
`trace:cleanse`
- To search for all issues that contain `cleanse` as part of any modifier, type the following:
`cleanse`
- To search for all suppressed vulnerabilities with `asdf` in the comments, type the following:
`suppressed:true comments:asdf`
- To search for all categories except for SQL Injection, type the following:
`category:!SQL Injection`

Performing Simple Searches

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

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



- To select a search term you used previously (during the current session), click the arrow in the search box, and then select a search term from the list. (After you exit the IDE, saved search terms are discarded.)


The Analysis Results window lists the query results (if any).


Performing Advanced Searches

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

Note: Advanced search is not available when you remediate audit results that are stored on Micro Focus Fortify Software Security Center.

To use the advanced search feature:

1. To the right of the search box, click the **Advanced Search** icon .
The Advanced Search dialog box opens.
2. From the first list on the left select a modifier.
If you plan to specify an unqualified search term, select **Any Attribute** from the modifier list.
3. From the middle list, select a comparison term.
4. In the combo box on the right, either type a search term, or select one from the list.
The search term list includes the known values in the current scan for the specified attribute. However, you can type any value into this field.
5. To add an AND or OR row to the query, click the **Add Criteria** icon.

6. To set the operator, click either the **AND** or **OR** button.
7. Specify the modifier, comparison term, and search term.
8. Add as many rows as you need for the search query.
9. To remove a row, to the right of the row, click **Delete** .
10. To remove all rows, at the bottom of the dialog box, click **Clear**.
11. To submit your completed search query, click **Find**.

Note: The **Find** button is only enabled after you create a complete search query.

Using the Audit Guide to Filter Issues

The Audit Guide wizard provides filtering of results.

To use the Audit Guide:

1. Select **Fortify > Audit Guide**.
The Audit Guide wizard opens.
2. Select the settings for the types of issues you want to display.
3. To use the advanced filtering options, click the **Advanced** tab.
 - In the **Audit Guide Filters** list, select the types of issues to filter out.
Click an issue type to see a description on the right side.
As you select items in the **Audit Guide Filters** list, the Fortify Extension for Visual Studio displays the filter details for this issue type below the **Audit Guide Filters** list and shows the number of issues found by each filter.
4. Click **OK** to apply your filtering selections.

Auditing Scan Results

The security team examines Fortify Project Results (FPR) and assigns values to custom tags associated with audit project issues during a code audit. The development team can then use these tag values to determine which issues to address and in what order.

To enable project auditing out of the box, Micro Focus Fortify Software Security Center provides a single default tag named **Analysis**. Valid values for the Analysis tag are Not an Issue, Reliability Issue, Bad Practice, Suspicious, and Exploitable. You can modify the Analysis tag attributes, revise the tag values, or add new values based on your auditing needs.

To refine your audit process, you can define your own custom tags. For example, you could create a 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.” For more information, see ["Configuring Custom Tags for Auditing" on page 40](#).

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

Note: Although you can add new custom tags 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 audit project (FPR) to Fortify Software Security Center.

Auditing Issues

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

1. Select the issue or group of issues in the Analysis Results window.
For information about the Analysis Results window, see ["Analysis Results Window" on page 17](#).
2. Read the abstract on the **Summary** tab, which provides high-level information about the issue, such as the analyzer that found the issue.
For example, "Command Injection (Input Validation and Representation, data flow)" indicates that this issue, detected by the Dataflow Analyzer, is a Command Injection issue in the Input Validation and Representation kingdom.
3. Click the **More Information** link or the **Details** tab to get more details about the issue.
4. On the **Summary** tab, assign an **Analysis** value to the issue to represent your evaluation.
5. Specify values for any custom tags as required by your organization.

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

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

Note: If you select a different value for **Analysis** than the **AA_Prediction** value set by Audit Assistant, and you select Include from the **AA_Training** list, then the next time the data is submitted to Audit Assistant, it updates the information used to predict whether or not an issue represents a true vulnerability. For more information about Audit Assistant, see the *Micro Focus Fortify Software Security Center User Guide*.

7. (Optional) In the **Comments** box, add any comments relevant to the issue and your evaluation.

Suppressing Issues

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

To suppress an issue, do one of the following:

- Select the issue in the Analysis Results window, and then click **Suppress** icon on the **Summary** tab.
- Right-click the issue in the Analysis Results window, and then select **Suppress**.

Viewing Suppressed Issues

To review results that have been suppressed:

- On the Analysis Results toolbar, select the **Visibility** menu  and then click **Show Suppressed Issues**.

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. In the Analysis Results window, select an issue.
2. In the Issue Auditing window, click the **Summary** tab, and then click **File Bug**.
If this is the first time you are submitting a bug, the Select Bugtracker Integration dialog box opens. Select the bug tracking application, and then click **Select**.
3. 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 product name, severity level, summary, and version.
4. Click **File Bug**.

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.

About Issue Templates

Micro Focus Fortify Static Code Analyzer produces comprehensive results for source code analysis. On large codebases, these results can be overwhelming. Issue templates provide features to sort and filter the results in ways that 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 issues into folders, which are logically defined sets of issues presented in the tabs on the Analysis Results window. You can further customize the sorting by providing 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 can 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 the audit. For example, you can use custom tags to track impact, severity, or priority of an issue using the same names and values used to track these attributes in other systems, such as a bug 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 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 a project uses the following order of preference:

1. The template that exists in the audit project.
2. The template `<sca_install_dir>\Core\config\filters\defaulttemplate.xml`
3. The template `<sca_install_dir>\Core\config\rules\defaulttemplate.xml`
4. The embedded Fortify default template

Saving Issue Templates

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, and the issue template is stored in the FPR when the project is saved. For information about how to change the issue template associated with an audit project, see ["Importing Issue Templates" on the next page](#).

Exporting Issue Templates

Exporting an issue template creates a file that contains the filter sets and custom tags for the current audit project. This is useful if you want to import the issue template into another audit project file.

To export an issue template:

1. Select **Fortify > Project Configuration**.
The Project Configuration dialog box opens.
2. Click the **Filter Sets** tab.
3. Click **Export Issue Template**.
4. Browse to the location where you want to save the file.
5. Type a file name without an extension, and then click **Save**.

The template settings are saved to the new XML file.

Importing Issue Templates

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

To import an issue template:

1. Select **Fortify > Project Configuration**.
The Project Configuration dialog box opens.
2. Click the **Filter Sets** tab.
3. Click **Import Issue Template**.
4. Select the issue template file to import.

The filter sets and custom tags are updated.

To revert to the default issue template settings, click **Reset Issue Template to Default**.

Configuring Custom Tags for Auditing

Custom tags enable auditors to set additional attributes that describe the issue. You can use custom tag values to filter and find issues.

The **Analysis** tag is configured by default and when you apply the **Analysis** tag to an issue, the icon in the Analysis Results issue list indicates the analysis status.

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.”


After you define a custom tag, the **Summary** tab displays it below the Analysis tag, which enables you to specify values as they relate to specific issues. The tag is 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.

Creating a Custom Tag


You can create custom tags to use when you audit results. Custom tags are saved as part of an issue template.

To create a custom tag:

1. Select **Fortify > Project Configuration**.
The Project Configuration dialog box opens.
2. Click the **Custom Tags** tab.

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

Note: Previously deleted tags are listed, and you can re-enable them. To create a new tag, click **Create New**.

4. In the Create New dialog box, type a name for the tag.
5. From the **Type** list, select the type of tag. The following tag types are available:
 - **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. To add a value for a list-type tag, do the following:
 - a. From the **Tags** list, select the tag.
 - b. Next to **Values**, click **Add Value** .
 - c. In the Add Value dialog box, type a value, and then click **OK**.
 - d. To use this value as the default for the new tag, select a value in the **Values** list, and then select **Default** on the right.
If no default is selected, the default value for the custom tag is empty.
 - e. To add a description for the value, type it in the **Description** box.
 - f. Repeat steps b through e until you have added all the tag values.
8. To add a description for any tag type:
 - a. From the **Tags** list, select the tag.
 - b. Type a description in the **Description** box on the right.


Deleting a Custom Tag

If you delete a custom tag, it is no longer available on the **Summary** tab and from the filter options.

Warning: If you delete a custom tag that was set for any issues, that tag and values are removed from the issue.

To delete a custom tag:

1. Select **Fortify > Project Configuration**.
The Project Configuration dialog box opens.
2. Click the **Custom Tags** tab.

3. Select the tag from the **Tags** list.
4. Next to **Tags**, click **Delete Tag** .

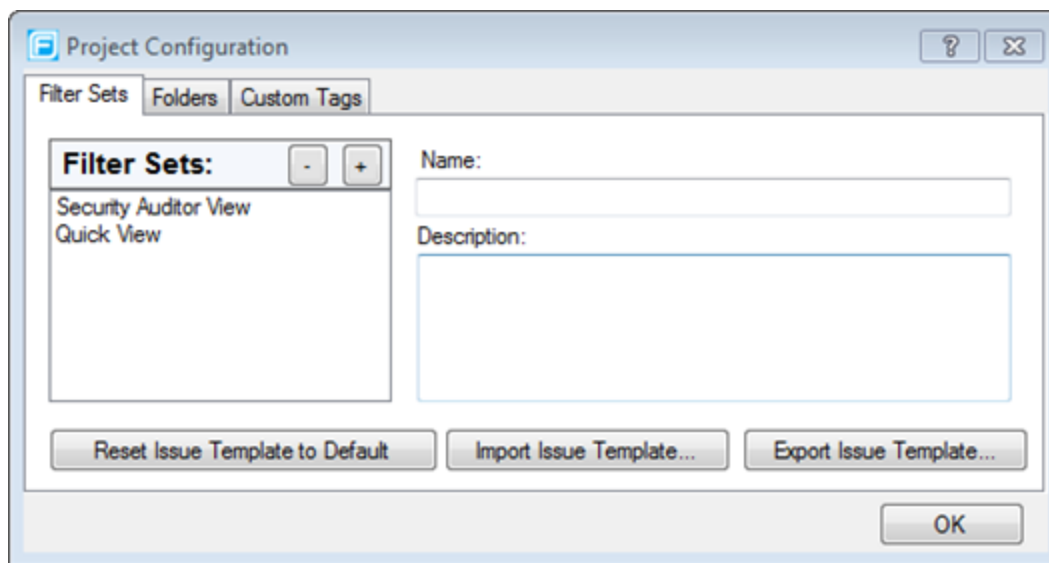
If you delete a tag that has an associated filter, you are prompted to also delete the filter.


Creating a Filter Set

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

To create a new filter set:

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



3. Next to **Filter Sets**, click **Create Filter Set** .
4. In the Create New Filter Set dialog box, type a name for the new filter set.
5. Select an existing filter set to copy, and then click **OK**.
6. To change the description of the new filter set, select it in the **Filter Sets** list, and then edit the text in the **Description** box on the right.

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 Analysis Results Window

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

Note: To find the filter that directed the issue to the folder, right-click the issue, and 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 Analysis Results window, select a filter set from the **Filter Set** list.
2. Right-click an issue, and then select **Generate Filter** from the shortcut menu.
The Create Filter dialog box opens and displays a list of suggested conditions.
3. To expand the conditions list, click **More Choices**.
4. Select the conditions to use in the filter. You can fine tune the filter later from the **Filter** tab.
5. To specify the type of filter you want to create, do one of the following:
 - 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 **Create New** to create a new folder.
A new folder is displayed only in this filter set.
6. Click **Create Filter**.
The new filter is placed at the end of the filter list. For folder filters, this gives the new filter the highest priority. Issues matching the new folder filter appear in the targeted folder.
7. To change the priority of a folder filter, drag the filter higher in the folder filter list.

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

Creating a Filter from the Filters Tab

Use the **Filters** tab option to create general filters for the attributes and values you want to filter. The filter is created in the selected filter set only.

Folder filters are applied in order and the issue is directed to the last folder filter it matches in the list. The wizard places your new filter at the end of the list.

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

1. From the **Filter Set** list, select a filter set.
2. Right-click **Visibility Filter** or **Folder Filter**, and then select **Create New Filter** from the shortcut menu.
3. From the first list, select an issue attribute.
4. From the second list, select a value to specify how to match the value.
The third list automatically displays the attribute values.
5. From the third list, select a value or specify a range as instructed in the **If** line.
6. 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 **Create New** to create a new folder.

The new filter displays at the end of the list. For folder filters, this gives the new filter the highest

priority. Issues that match the new folder filter are displayed in the targeted folder.

7. To change the priority, drag the filter higher in the folder filter list.

The issues are sorted based on the new filter.

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

Copying a Filter to Another Filter Set

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

To copy a filter:

1. From the **Filter Set** list, select a filter set.
2. On the **Filters** tab, right-click a filter, and then select **Copy Filter To** from the shortcut menu.
The Select a Filter Set dialog box lists the filter sets.
3. Select a filter set, and then click **OK**.
The filter is added to the destination filter set in the last position.
4. To change the order of the folder filters, drag and drop the filters in the list.

Managing Folders

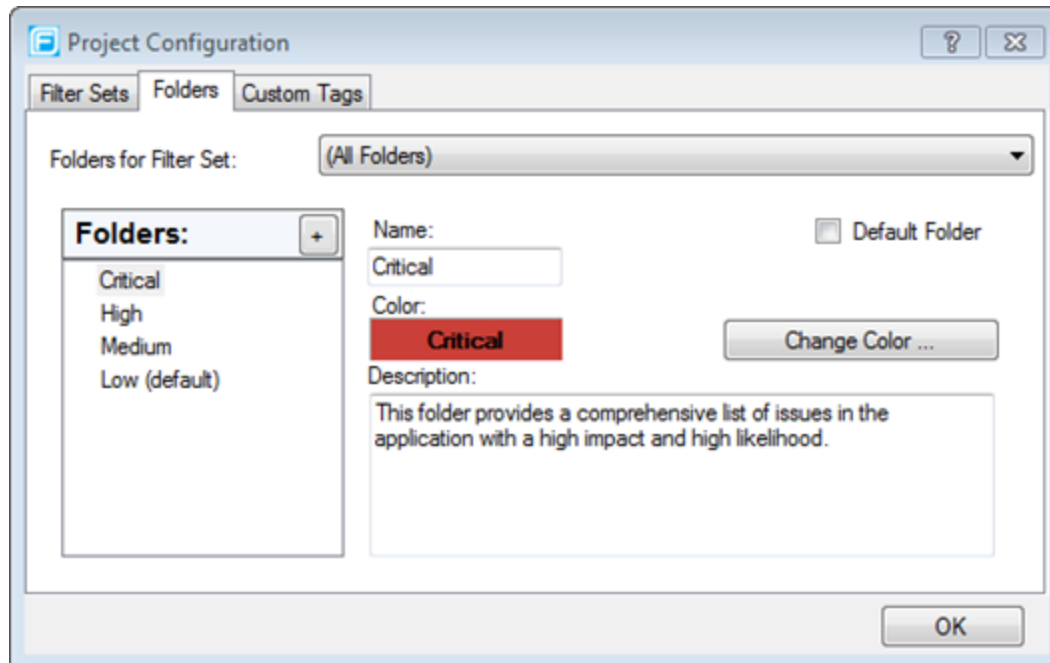
Folders are logical sets of issues that are defined by the filters in the active filter set. Even though a folder can appear in more than one filter set, the contents might differ depending on the filters in that filter set that target the folder. To accommodate filter sets that attempt to provide sorting mechanisms that have little overlap, it is possible to have filter sets with different folders. Folders are defined without any relation to the filter sets in which they might appear.

Creating a Folder

You can add a new folder to a filter set so that you can display a group of issues you have filtered to the folder.

To create a folder:


1. Select **Fortify > Project Configuration**.
The Project Configuration dialog box opens.
2. Click the **Folders** tab.
Currently defined folders are listed on the left. Fields that indicate the name, color, and description of the selected folder are on the right.



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

This selection updates the **Folders** list to display folders associated with the selected filter set.

4. To add a folder:

- a. Next to **Folders**, click **Create Folder** .

The Create New Folder dialog box opens.

- b. Type a unique name for the new folder, select a folder color, and then click **OK**.

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

5. To sort all issues that do not match a folder filter into this folder, select **Default Folder**.
6. Click **OK**.


The new folder is added to the local issue template. The folder displays as a tab with the other folders in the **Analysis Results** window.

Note: To display issues in this folder, create a folder filter that targets the new folder (see ["Creating a Filter from the Analysis Results Window" on page 42](#) and ["Creating a Filter from the Filters Tab" on page 43](#)).

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 only appears in the selected filter set using the instructions in ["Creating a Folder" on the previous page](#). To display issues in this folder, create a folder filter that targets the new folder.

To add a folder to a filter set:

1. Select **Fortify > Project Configuration**.
The Project Configuration dialog box opens.
2. Click the **Folders** tab.
3. From the **Folder for Filter Set** list, select a filter set to which you want to add an existing folder.
This selection updates the **Folders** list to display folders associated with the selected filter set.
4. Next to **Folders**, click + .
The Enable New Folder to the Filter Set dialog box opens. If all folders are already associated with the selected filter set, the Create New Folder dialog box opens.
5. Select the folder to add, and then click **Select**.
The selected folder is listed.
6. Click **OK**.
The folder is displayed as a tab with the other folders in the **Analysis Results** window.

Renaming a Folder

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

To rename a folder:

1. Select **Fortify > Project Configuration**.
The Project Configuration dialog box opens.
2. Click the **Folders** tab.
3. From the **Folders for Filter Set** list, select a filter set that displays the folder you want to rename.
4. Select the folder in the **Folders** list.
The folder properties are displayed on the right.
5. In the **Name** box, type the new folder name.
6. Click **OK**.

The tab displays the new folder name.

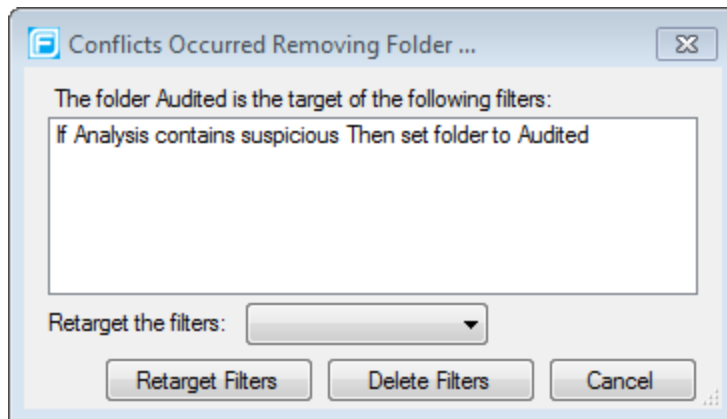
Removing a Folder

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

To remove a folder:

1. Select **Fortify > Project Configuration**.
2. Click the **Folders** tab.
3. From the **Folders for Filter Set** list, select a filter set that contains the folder you want to remove.
The folders in the selected filter set are listed.

- Next to **Folders**, select the folder, and then click -.
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:

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

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

The folder is no longer displayed as a tab.

Scan Results Reports

The following topics provide information about generating BIRT and legacy reports for your scan results, and how to work with legacy Fortify report templates.

About BIRT Reports

The following table describes the BIRT reports available.

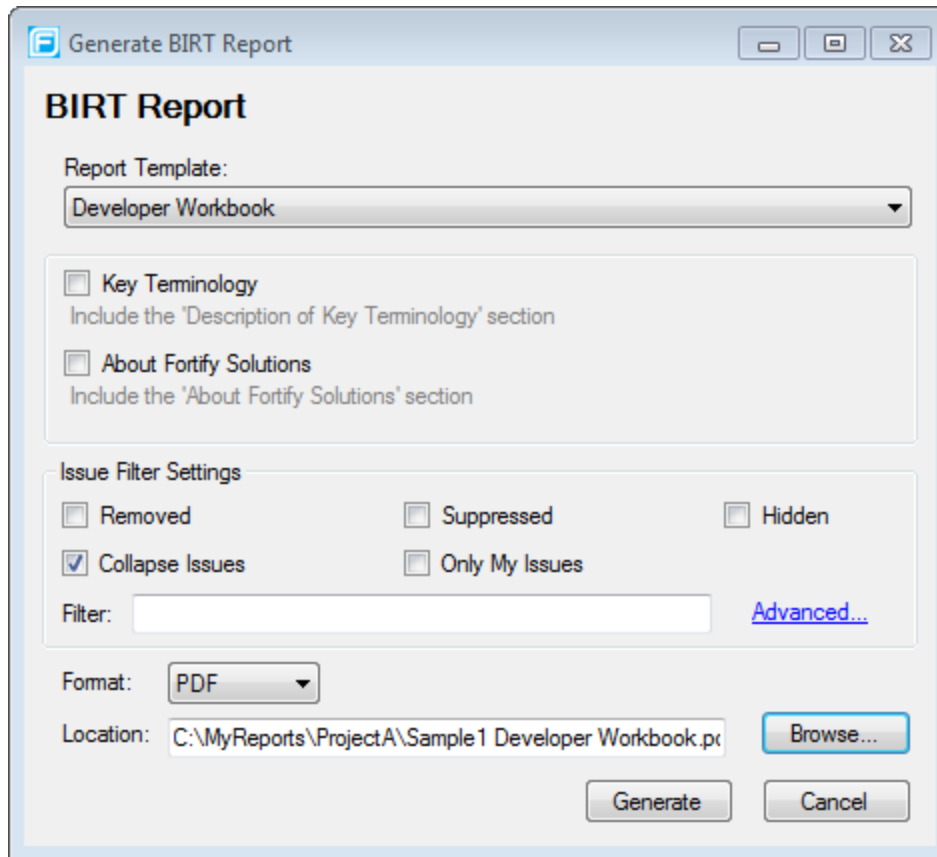
Report Template	Description
CWE/SANS Top 25	This report details findings related to the CWE/SANS Top 25 most dangerous programming errors uncovered and provides information about where and how to address the findings.
Developer Workbook	This report, which is targeted at project managers and developers, contains all of the information needed to understand and fix issues discovered during an audit.

Report Template	Description
DISA CCI 2	This report provides a standard identifier for policy based requirements which connect high-level policy expressions and low-level technical implementations. The status of a CCI is considered "In Place" when there are no issues reported for a given CCI. If the project is missing a Fortify Static Code Analyzer scan, or the scan contains findings that have not been fixed, hidden or suppressed, CCI-003187 is not considered "In Place." Similarly, if the project is missing a Micro Focus Fortify WebInspect scan, or the scan contains any critical findings, CCI-000366 and CCI-000256 are not considered "In Place."
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.
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 report:

1. Select **Fortify > Generate BIRT Report**.
 The Generate BIRT 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 you want to include in the report.

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

- a. To include detailed descriptions of reported issues, select the **Detailed Report** check box.
 - b. To categorize issues by Fortify Priority instead of folder names, select the **Categories By Fortify Priority** check box.
 - c. To include Description of Key Terminology in the report, select the **Key Terminology** check box.
 - d. To include the About Fortify Solutions section in the report, select the **About Fortify Solutions** check box.
5. To filter information from the report, select the optional issue filter settings 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 30](#).
6. Click the **Format** menu to select 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 location.
8. Click **Generate**.
9. If a report with the same file name already exists, you are prompted to either:
 - Click **No** to overwrite the existing report.
 - Click **Yes** to have the report saved to a file with a sequential number appended to the file name (for example: Sample1_DISA_STIG(1).pdf).

About Legacy Reports

The legacy reports include user-configurable report templates. Report templates provide several optional sections and subsections that gather and present specific types of data. The following sections provide information about the default reports and report templates, instructions on how to modify existing reports, and how to create your own reports.

Running Legacy Reports

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

To run a report:

1. Select **Fortify > Generate Legacy Report**.
The Generate Legacy Report dialog box opens.
2. From the **Report** list, select a report template.
3. (Optional) Change the report section settings.
4. Click **Print Report**.
5. Specify a file name and a location to save the report.
6. Select the report file format (PDF, RTF, or XML).
7. Click **Save**.

Opening Legacy Report Templates

To open a report template:

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

The report template settings display in the Generate Legacy Report dialog box.

Legacy Report Templates

This section provides information about how to select and edit a legacy report template. If you or another user have edited or created additional legacy report templates, you might not see the default report templates as 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. It also gives a high-level summary of the number of issues in each category.
- **Fortify Security Report**—This report, which is designed for project managers, includes comprehensive analysis information and high-level audit details (if the auditor provided these). The Fortify Security Report also provides a high-level description and examples of categories that are of the highest priority.
- **Fortify Scan Summary**—Provides high-level information based on the category of issues that Micro Focus Fortify Static Code Analyzer found as well as a project summary and a detailed project summary
- **OWASP Top Ten <year>**—Provides a high-level summary of vulnerabilities. These reports organize vulnerabilities on the top ten issues identified by the Open Web Security Project (OWASP) in the respective year. This report type includes report overview, issues broken down by OWASP top ten, and results outline sections.

Selecting Legacy Report Sections

You can choose which sections to include in the report.

To select the sections to include in a report:

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

The section details display in the right side of the dialog box. For details on how to edit each section, see ["Editing Legacy Report Subsections" below](#).

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

Editing Legacy 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. The following sections describe how to perform these tasks:

Editing Text Subsections

To edit a text subsection:

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

2. Click **Edit**.

The text box displays the text and variables to be included in the report.

3. Edit the text and text variables.

As you edit text subsections, you can insert variables that are defined when you run the report. These variables are described in the following table.

Variable	Description
\$AUDIT_GUIDE_SUMMARY\$	List of filters created with answers to Audit Guide Wizard questions
\$CLASSPATH_LISTINGS\$	JAR files used during scan, one relative path per line
\$COMMANDLINE_ARGS\$	Complete list of command-line options (same format as project summary)
\$FILE_LISTINGS\$	List of files scanned, each file in the following format: <relative_file_path> # Lines # kb <timestamp>
\$FILTERSET_DETAILS\$	List of filters used by the current filter set
\$FILTERSET_NAME\$	Name of the current filter set
\$FORTIFY_SCA_VERSION\$	Micro Focus Fortify Static Code Analyzer version
\$LIBDIR_LISTINGS\$	Libdirs specified during scan, one relative path per line
\$LOC\$	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 during analysis phase (same format as project summary)
\$RESULTS_CERTIFICATION\$	Complete certification detail with list of validity on a per file basis (see project summary)
\$RESULTS_	Short certification description (same format as project summary)

Variable	Description
CERTIFICATION_SUMMARY\$	
\$RULEPACKS\$	Complete list of Rulepacks used during analysis (same format as project summary)
\$RUN_INFO\$	Content from the Project Summary Runtime Information tab
\$SCAN_COMPUTER_ID\$	Hostname of the machine on which the scan was performed
\$SCAN_DATE\$	Date of analysis with the default formatting style for the locale
\$SCAN_SUMMARY\$	Summary of codebase scanned in format # files, # lines of code
\$SCAN_TIME\$	Time of analysis phase
\$SCAN_USER\$	User name of 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
\$VERSION_LABEL\$	Label of the scanned project (available only if the Fortify Static Code Analyzer -build-label option was used in the scan)
\$WARNINGS\$	Complete list of warnings issued (same format as 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 is displayed below the subsection title.
2. Click the issues list heading to expand the options.
3. Select the attributes used to group the results list.
If you group by category, the recommendations, abstract, and explanation for the category are also included in the report.
4. (Optional) Refine the issues shown in this subsection by using the search function
For more details about the search syntax, see "[Searching for Issues](#)" on page 29.

Editing Chart Subsections

To edit a chart subsection:

1. Select the check box next to the subsection title to include this text in the report.
A chart description is displayed below the subsection title.
2. Select the attributes used to group the chart data.
3. (Optional) Refine the issues shown in this subsection with the search function.
For information about search syntax, see ["Searching for Issues" on page 29](#).
4. Select the chart format (table, pie, or bar).

Saving Legacy Report Templates

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

To save settings as a report template:

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

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

Saving Changes to Legacy Report Templates

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

To save changes to a report template:

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

Editing Legacy 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 the report template XML files is `<sca_install_dir>\Core\config\reports`.

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

Adding Legacy 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 section contents 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 this example, the `Results Outline` section contains two subsections. The first is a text subsection titled `Overall number of results`. The second subsection is a results list titled `Vulnerability Examples by Category`. A section can contain any combination of subsections.

Adding Report Subsections

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

Adding Text Subsections

In a text subsection, you can include the `Title` tag, the `Description` tag, and the `Text` tag. In the `Text` tag, you can provide the default content although the user can edit the content before generating a report. For a description of the text variables available to use in text subsections, see ["Editing Legacy](#)

[Report Subsections" on page 51](#). The following XML is the Overall number of results subsection in the Results Outline section:

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

In this example, the text subsection is titled Overall number of results. The text that describes 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 the user can edit the content before they generate a report. To generate a results list, the Chart tag attribute chartType is set to list. You can also include 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 text used 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 value of the Axis tag) where there are issues matching 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 the user can edit the content before generating a report. To generate a pie chart, set the Chart tag

attribute `chartType` to `pie`. The options are `table`, `pie`, and `bar`. The user can change this setting before generating 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 following issues have been discovered since the last scan.` This chart includes all issues (the `Refinement` tag is empty) and groups the issues based on the value of `New Issue` (the value of the `Axis` tag). A pie chart (`chartType="pie"`) is displayed.

Working with Audit Projects

This section provides information about how to open an audit project, migrate audit data, merge audit data, audit projects collaboratively, and upload audit results to Micro Focus Fortify Software Security Center.

Opening Audit Projects

To open an audit project file:

1. Open a solution or project.
2. Select **Fortify > Open Audit Project**.
3. Browse to and select an audit project file (FPR, FVDL, or XML).
4. Click **Open**.
5. If the source code is not available in the FPR, you are prompted to select the root directory for your project's source code. Select the root directory, and then click **OK**.

The Fortify Extension for Visual Studio displays the project in the auditing interface.

About Merging Audit Data

You can merge audit data into your project from another file. Audit data includes the custom tags and comments that were added to an issue. Comments are merged into a chronological list, while the custom tag values are updated.

Note: Issues are not merged. Only the newer scanned issues are shown. Issues in the older file that are not in the newer file are marked as removed and hidden by default.

Make sure that the projects you merge contain the same analysis information, that the scan was on the same source code (no missing libraries or files), the Micro Focus Fortify Static Code Analyzer options were the same, and the scan was performed with the same set of Secure Coding Rulepacks and custom Rulepacks.

Merging Audit Data

To merge audit projects:

1. Open an audit project in Visual Studio.
2. Select **Fortify > Merge Audit Projects**.
The Select Audit Project dialog box opens.
3. Select an audit project (FPR, FVDL, or XML file), and then click **Open**.
The audit projects are merged.
4. To confirm the number of issues added or removed from the file, click **OK**.

Note: If the scan is identical, the process does not add or remove issues.

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

Performing a Collaborative Audit

You can audit a project on Micro Focus Fortify Software Security Center collaboratively with other Fortify Software Security Center users.

To start a collaborative audit:


1. If necessary configure a connection to Fortify Software Security Center:
 - a. Select **Fortify > Options**.
 - b. Click **Server Configuration**.
 - c. Under **Software Security Center Configuration**, specify the **Server URL** for Fortify Software Security Center (for example, `http://111.0.0.1:8181/ssc`).
 - d. If necessary, specify the proxy server and port number.
 - e. Click **OK**.
2. Select **Fortify > Open Collaborative Audit**.

If you already have an audit project open, close it.

3. If prompted, type your Fortify Software Security Center login credentials:
 - a. From the **Login Method** menu, select the login method set up for you on Fortify Software Security Center.
 - b. To save your login information, select the **Save Login Method** check box.

The Fortify Extension for Visual Studio saves your login information for all future use of this extension until you install a new Fortify Extension for Visual Studio.

- c. Depending on the login method you selected, do one of the following:

Login Method	Procedure
Username/Password	Type your Fortify Software Security Center username and password.
X.509 SSO	Fortify Software Security Center must be configured to use X.509 Certification-based SSO. <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p>Note: Your certificate must be located in the current user certificate store and in the Personal store.</p> </div> <ol style="list-style-type: none"> i. Click Browse for Certificate . ii. Select the certificate for the sign-on, and then click OK.
Kerberos SSO	Fortify Software Security Center must be configured to use SPNEGO-based Kerberos authentication. No additional information is required.

- d. Click **OK** to connect to Fortify Software Security Center.
4. In the Download Collaborative Audit dialog box, select an application version, and then click **Select**.
 The Fortify Extension for Visual Studio downloads the audit project file from Fortify Software Security Center and opens it in the auditing interface.
5. Audit the project as described in ["Auditing Issues" on page 37](#).
6. When you have completed the audit, select **Fortify > Upload Audit Project**.

Note: If necessary, update your audit permission settings from Fortify Software Security Center by selecting **Fortify > Refresh Permissions**.

Uploading Results to Fortify Software Security Center

To upload results to Micro Focus Fortify Software Security Center:

1. If necessary configure a connection to Fortify Software Security Center:
 - a. Select **Fortify > Options**.
 - b. Click **Server Configuration**.
 - c. Under **Software Security Center Configuration**, specify the **Server URL** for Fortify Software Security Center (for example, `http://111.0.0.1:8181/ssc`).
 - d. If necessary, specify the proxy server and port number.
 - e. Click **OK**.
2. Select **Fortify > Upload Audit Project**.
3. If necessary, type your Fortify Software Security Center credentials.
The Upload Audit Project dialog box lists the current applications.
4. Select an application version, and then click **Select**.

Note: If you are working on a collaborative audit for an application you just downloaded, then the audit project is automatically uploaded to the same application version. You are not prompted to select an application.

About Updating Security Content

To optimize the Fortify Extension for Visual Studio functionality to scan with Micro Focus Fortify Static Code Analyzer, you must have complete and up-to-date security content. First configure how you plan to obtain security content updates (see ["Configuring Security Content Updates" on the next page](#)). Then you can obtain the latest security content by doing one of the following:

- ["Updating Security Content" on the next page](#)
- ["Scheduling Automatic Security Content Updates" on the next page](#)
- ["Manually Updating Security Content" on page 62](#)

Note: When you update security content, the previous security content files are overwritten.

You can also import custom rules from the Fortify Extension for Visual Studio (see ["Importing Custom Rules" on page 62](#)).

Configuring Security Content Updates

Before you update security content, configure the server information to use for security content updates. To update security content manually (without an Internet connection or Micro Focus Fortify Software Security Center), see ["Manually Updating Security Content" on the next page](#).

To configure the security content update server:

1. Select **Fortify > Options**.
The Options dialog box opens to the **Server Configuration** section.
2. Under **Security Content Update**, select one of the following:
 - To update security content from your Fortify Software Security Center instance, select the **Update Security Content from Software Security Center** check box.
 - To specify an update server from which to update security content, select the **Use Custom Server Settings** check box.
3. If you selected the **Use Custom Server Settings** check box, do the following:
 - a. In the **Server URL** box, type the URL for the update server.
 - b. If required, in the **Proxy Server** and **Port** boxes, type the proxy server and port number, respectively.

Updating Security Content

To update security content from the update server:

1. Select **Fortify > Options**.
2. In the left panel, select **Security Content Management**.
3. Click **Update**.
If new content is available, it is updated and listed under **Installed Fortify Security Content**.
4. Click **OK**.

Scheduling Automatic Security Content Updates

To schedule automatic security content updates:

1. Select **Fortify > Options**.
2. In the left panel, select **Server Configuration**.
3. Under **Security Content Update**, select the **Update security content automatically** check box.
4. In the **Update Frequency (Days)** box, specify how often the security content is to be updated, and then click **OK**.

Manually Updating Security Content

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

To manually update the security content:

1. Open a command prompt, and then navigate to the `<sca_install_dir>\bin` directory.
2. Type `fortifyupdate.cmd -import <file>.zip`.

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

Importing Custom Rules

You can import custom rules to use in your scans. Fortify Extension for Visual Studio imports custom rules to the `<sca_install_dir>\Core\config\customrules` directory.

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

To import custom rules:

1. Select **Fortify > Options**.
2. In the left panel, select **Security Content Management**.
3. Click **Import**.
The Select Security Content dialog box opens.
4. Browse to and select a `*.xml` or `*.bin` file to import.
The imported file is listed under **Installed Custom Security Content**.
5. Click **OK** to close the Options dialog box.

Integrating with a Bug Tracker Application

The Fortify Extension for Visual Studio provides a plugin interface to integrate with bug tracker applications. This enables you to file bugs directly from the Fortify Extension for Visual Studio.

If you installed the samples with the Static Code Analyzer and Applications installation, an example plugin exists for Bugzilla. You can select the bug tracker plugin with the dialog box that opens when you file your first bug.

Filing Bugs to Team Foundation Server

The Fortify Extension for Visual Studio supports integration with bug tracker applications so that you can file bugs directly to Team Foundation Server (TFS).

To file a bug to TFS:

1. Open an audit project in Visual Studio.
2. In the Analysis Results window, select an issue.
3. In the Issue Auditing window, click the **Summary** tab, and then click **File Bug**.
4. If this is the first time you have filed a bug to TFS, the Select Bugtracker Plugin dialog box opens. Do the following:
 - a. Select **Team Foundation Server Plugin**, and then click **Select**.
 - b. In the Connect to Team Foundation Server dialog box, select a server, and then click **Connect**.
5. Specify the following information for your TFS installation:
Project: *<project_name>*
WorkItem Type: **Bug**
6. Click **OK**.
7. (Optional) In the Team Foundation Server Plugin dialog box, provide the information to file the bug report.
8. Click **File Bug**.

Using the Debug Option

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

To enable debugging:

1. Navigate to the *<sca_install_dir>\Core\config* directory and open the *fortify.properties* file in a text editor.
2. You can either enable debug mode for all Fortify Software components or for specific components. Remove the comment tag (#) from in front of the property and set the value to true.

Property	Description
<code>#com.fortify.Debug=false</code>	If set to true, all the Fortify Software components run in debug mode.
<code>#com.fortify.VS.Debug=false</code>	If set to true, the Fortify Extension for Visual Studio runs in debug mode.

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

- `C:\users\<username>\AppData\Local\Fortify\sca<SCAVersion>\log`
- `C:\users\<username>\AppData\Local\Fortify\VS<VSVersion>-<SCAVersion>\log`

Chapter 3: Remediating Results from Fortify Software Security Center

You can download audit results for your code from Micro Focus Fortify Software Security Center so that you can resolve security-related issues in Visual Studio.

This section contains the following topics:

Connecting to Fortify Software Security Center	64
Working with Applications	64
Working with Issues	67

Connecting to Fortify Software Security Center

Before you can access the audit results on Micro Focus Fortify Software Security Center, you need to configure your connection to Fortify Software Security Center.

To connect to Fortify Software Security Center:

1. Select **Fortify > Remediation Options**.
The Remediation Options window opens.
2. On the **Server** tab, type the URL for your Fortify Software Security Center server, and then click **OK**.

If you are running the server on your local machine with port 8180, leave the default URL (<http://localhost:8180/ssc>). Otherwise, substitute your Fortify Software Security Center IP address for `localhost` and your port number for 8180.

For information on how to access audit results on Fortify Software Security Center, see "[Connecting to a Fortify Software Security Center Application](#)" on the next page.

Working with Applications

Applications in Micro Focus Fortify Software Security Center provide the security issues related to a specific application. Applications organize these issues into folders based on filters.

Folders contain logically defined sets of issues. For example, you can group all critical issues for a project into a Critical folder. Likewise, you can group all low-priority issues for the same audit project into a Low folder.


Filters determine which issues are visible in the user interface. The filters are organized into filter sets. 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 issues.

Connecting to a Fortify Software Security Center Application

After you have configured a connection to Micro Focus Fortify Software Security Center (see ["Connecting to Fortify Software Security Center" on the previous page](#)), you can select an application.

To select an application:

1. Select **Fortify > Connect to SSC**.
2. If prompted, type your Fortify Software Security Center login credentials:
 - a. From the **Login Method** menu, select the login method set up for you on Fortify Software Security Center.
 - b. To save your login information, select the **Save Login Method** check box.
The Fortify Extension for Visual Studio saves your login information for all future use of this extension until you install a new Fortify Extension for Visual Studio.
 - c. Depending on the login method you selected, do one of the following:

Login Method	Procedure
Username/Password	Type your Fortify Software Security Center username and password.
X.509 SSO	<p>Fortify Software Security Center must be configured to use X.509 Certification-based SSO.</p> <div style="background-color: #f0f0f0; padding: 5px;"> <p>Note: Your certificate must be located in the current user certificate store and in the Personal store.</p> </div> <ol style="list-style-type: none"> i. Click Browse for Certificate . ii. Select the certificate for the sign-on, and then click OK.
Kerberos SSO	Fortify Software Security Center must be configured to use SPNEGO-based Kerberos authentication. No additional information is required.

- d. Click **OK** to connect to Fortify Software Security Center.
3. In the Select Application Version dialog box, select the application version you want to open, and then click **OK**.

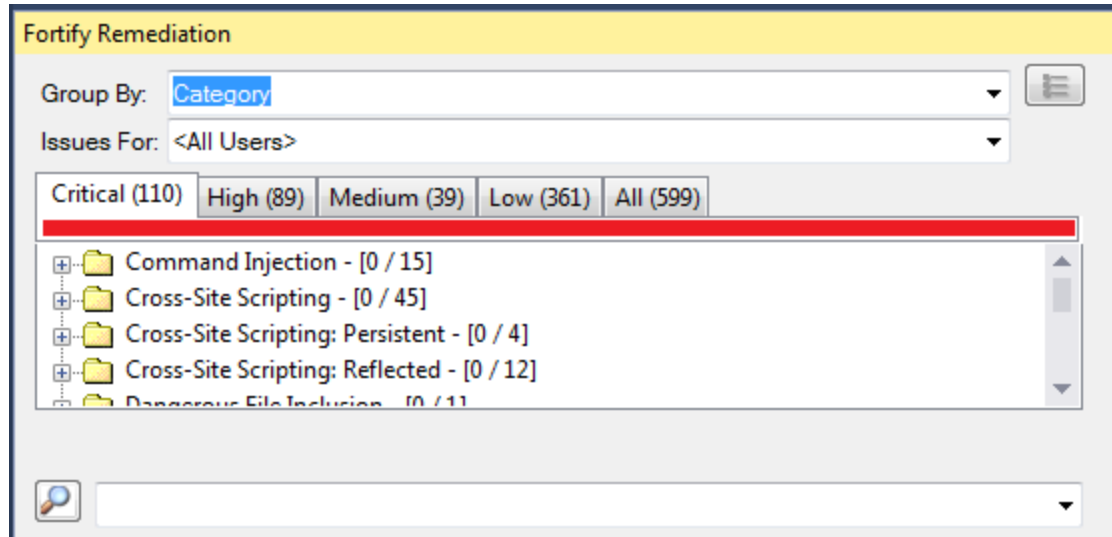
The Fortify Extension for Visual Studio sends a request to Fortify Software Security Center and downloads the results for the application version you selected.

Viewing and Selecting Issues in an Application

When you connect to a Micro Focus Fortify Software Security Center application, the Fortify Extension for Visual Studio downloads the issues for that application version. Fortify Software Security Center

provides a number of default folder types. Your view might be different, depending on whether your organization has created custom folders.

1. In the Fortify Remediation view, click the **Filter** icon  to the right of the **Group By** list, and then select **Filter Set**.



2. Select a filter to apply:
 - Select **Security Auditor View** to list all issues relevant to a security auditor.
 - Select **Quick View** to list only 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).

Note: You might see different filter sets depending on the filter sets associated with the application.

3. From the **Group By** list, select a value to use to sort issues in all visible folders into groups. The default grouping is **Category**. For a description of the **Group By** options, see "[Grouping Issues](#)" on page 27.
4. From the **Issues For** list, select one of the following:
 - **<All Users>**
 - Your Fortify Software Security Center user name. This is the default.
5. Click one of the following category tabs (folders).
 - The **Critical** tab contains issues that have a high impact and a high likelihood of exploitation. Fortify recommends that you remediate critical issues immediately.
 - The **High** tab contains issues that have a high impact and a low likelihood of exploitation. Fortify recommends that you remediate high issues with the next patch release.
 - The **Medium** tab contains issues that have a low impact and a high likelihood of exploitation. Fortify recommends that you remediate medium issues as time permits.

- The **Low** tab contains issues that have a low impact and a low likelihood of exploitation. Fortify recommends that you remediate low issues as time permits (your organization can customize this category).
- The **All** tab contains all issues.

The tabs display issues based on your **Group By**, **Issues For**, and **Filter** selections. After you select a tab, the Fortify Extension for Visual Studio retrieves the issues from Fortify Software Security Center.

6. Select an issue to view.

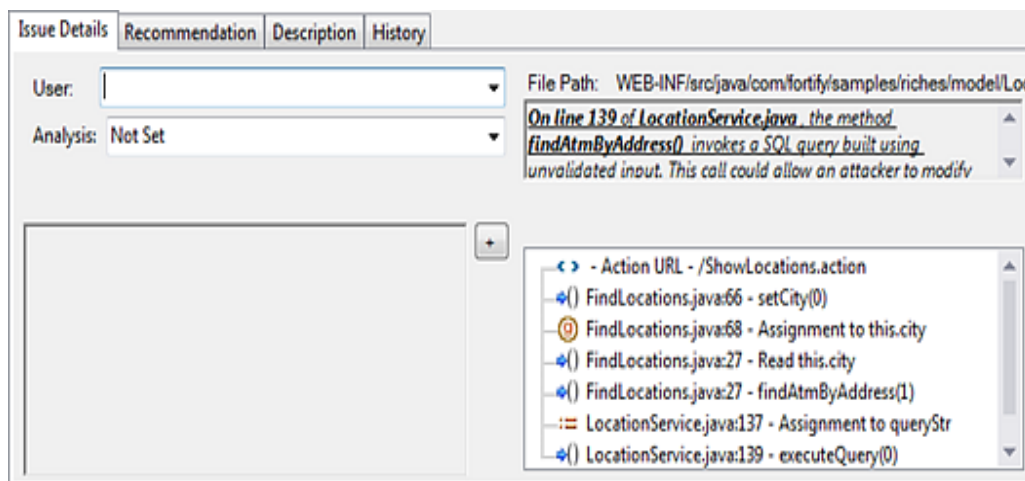
Working with Issues

After you select an issue, the Fortify Extension for Visual Studio provides issue-specific content organized in the Fortify Remediation window into the **Issue Details**, **Recommendation**, **Description**, and the **History** tabs.

This section provides descriptions of these tabs and their components.


Issue Details Tab

The **Issue Details** tab provides a dashboard for issues.



The following table describes the **Issue Details** tab.

Tab Element	Description
User	Select a name from this list to assign a user to the selected issue.
Analysis	Displays the analysis type for the selected issue. To change the analysis type, select an item from the list.

Tab Element	Description
<custom_tagname>	<p>Any custom tags your organization has defined in Micro Focus Fortify Software Security Center. If available, these are displayed below the Analysis list.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>For more information about Audit Assistant, see the <i>Micro Focus Fortify Software Security Center User Guide</i>.</p>
File Path (top right)	The path to the location of the source file for the selected issue.
Issue Abstract (top right)	Displays a summary of the selected issue.
Analysis Evidence (bottom right)	Lists the items of evidence that the analyzer uncovered. Evidence is presented in the order it was discovered. For information about the Analysis Evidence icons, see " Analysis Evidence Window " on page 20.
Comments (bottom left)	<p>Displays any comments added to the issue.</p> <p>To add a comment to the selected issue:</p> <ol style="list-style-type: none"> 1. Click Add Comment . 2. Type a comment, and then click OK.

Recommendation Tab

The **Recommendation** tab provides suggestions and examples that show how to secure a vulnerability or remedy a bad practice. The following table describes the tab sections.

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

Description Tab

The **Description** tab provides an abstract of the selected issue. It might also provide more detailed explanations, including examples with descriptive text and code samples. The following table describes the tab sections.

Section	Description
Abstract/Custom Abstract	Displays a summary description of the selected issue, including custom abstracts defined by your organization
Explanation/Custom Explanation	Displays a description of the conditions under which an issue of the selected type occurs. This includes a discussion of the vulnerability, the constructs typically associated with it, ways in which it can be exploited, and the potential ramifications of an attack. This section also provides custom explanations defined by your organization.
Instance ID	Unique identifier for an issue
Primary Rule ID	Primary rule that found the issue
Priority Metadata Values	Priority metadata values for an issue
Legacy Priority Metadata Values	Legacy priority metadata values for an issue

History Tab

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

Customizing Issue Visibility

You can customize the Fortify Remediation window to determine which issues it displays.

1. Select **Fortify > Remediation Options**.

The Remediation Options dialog box opens.

2. Click the **Issue Visibility** tab.

3. Select or clear the following check boxes:

- To display all hidden issues, select **Show Hidden Issues**.

Note: The visibility filter settings in the issue template associated with the application version determine which issues are hidden.

- To display all issues that were detected in the previous analysis, but no longer exist, select **Show Removed Issues**.

Note: Users who audit issues can suppress specific types of issues that are not considered high priority or of immediate concern. For example, auditors can suppress issues that are fixed, or issues that your organization plans not to fix.

- To display all suppressed issues, select **Show Suppressed Issues**.

4. Click **OK**.

Searching for Issues

You can use the search box below the issues list in the **Analysis Results** window to search for issues. For detailed instructions about the search capabilities, see ["Searching for Issues" on page 29](#).

Assigning Users to Issues

The **User** list contains all of the users for the application version, and also a blank value. Use the blank value to unassign a user from an issue.


1. From the issues list in the Fortify Remediation window, select an issue.
2. Select the **Issue Details** tab and select a user from the **User** menu.


The Fortify Extension for Visual Studio updates the application on the Micro Focus Fortify Software Security Center server.

Assigning Tags to Issues

To assign tag values to an issue:

1. From the issues list in the Fortify Remediation window, select an issue.
2. From the **Analysis** list on the **Issue Details** tab, select a value that reflects your assessment of this issue.
3. If custom tags defined for the project exist, provide values for them.

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

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

Locating Issues in Source Code

Because the Fortify Extension for Visual Studio works as an extension to your Visual Studio IDE, you can use it to locate security-related issues in your code. You must have the same project open in both Visual Studio and the Fortify Extension for Visual Studio.

To locate an issue in the source code, do either of the following:

- From the issues list in the Fortify Remediation window, select an issue.
- From the **Issue Details** tab, select an issue from the Analysis Evidence list.

The Fortify Extension for Visual Studio jumps to the line of code that contains the security-related issue displayed in Visual Studio.

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 (Fortify Extension for Visual Studio 19.1.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!