

OpenText™ Fortify Extension for Visual Studio

Software Version: 25.2.0

User Guide

Document Release Date: May 2025

Software Release Date: May 2025

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 2009 - 2025 Open Text.

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

Trademark Notices

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

Documentation updates

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

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

This document was produced on May 28, 2025.

Contents

Preface	7
Contacting Customer Support	7
For More Information	7
Product feature videos	7
Change Log	8
Chapter 1: Introduction	10
Product name changes	10
Fortify Extension for Visual Studio	10
Fortify Security Content	11
Installing Fortify Extension for Visual Studio	11
Related documents	12
All products	12
Fortify ScanCentral SAST	13
Fortify Software Security Center	13
OpenText SAST	14
OpenText Application Security Tools	15
Chapter 2: Using the Fortify Extension for Visual Studio	16
About Analyzing the Source Code	16
Requirements for Analyzing Source Code	17
Working with Fortify Software Security Center	18
Configuring a Connection to Fortify Software Security Center	18
Logging in to Fortify Software Security Center	18
Synchronizing with Fortify Software Security Center	20
About Scanning Locally	21
Configuring Security Content Updates	21
Updating Security Content	23
Importing Custom Security Content	24
About Quick Scan Mode	24
Configuring Local Scan Options	25

Configuring Advanced Local Scan Options	26
Scanning Projects or Solutions Locally	28
About Scanning with Fortify ScanCentral SAST	28
Configuring Fortify ScanCentral SAST Options	30
Scanning Projects or Solutions with Fortify ScanCentral SAST	32
Advanced Scanning of Solutions with Fortify ScanCentral SAST	33
Viewing Analysis Results	34
Analysis Results Window	35
Filter Sets	35
Folders (Tabs)	36
Group By List	36
Customizing the Issues Display	36
Viewing Project Summary Information	37
Analysis Trace Window	38
Issue Auditing Window	40
Code Editor	45
Grouping Issues	46
Creating a Custom Group By Option	47
Searching for Issues	48
Performing Advanced Searches	48
Search Syntax	49
Search Modifiers	50
Search Query Examples	55
Filtering Issues with the Audit Guide	56
Auditing Analysis Results	57
Auditing Issues	58
Suppressing Issues	59
Submitting an Issue as a Bug	59
Using Issue Templates	59
Saving Issue Templates	60
Exporting Issue Templates	60
Importing Issue Templates	61
Configuring Custom Tags for Auditing	61
Adding a Custom Tag	62
Hiding a Custom Tag	63
Creating a Filter Set	64
Creating a Filter from the Analysis Results Window	65

Creating a Filter from the Filters Tab	65
Copying a Filter to Another Filter Set	66
Managing Folders	67
Creating a Folder	67
Adding a Folder to a Filter Set	68
Renaming a Folder	69
Removing a Folder	69
Generating Analysis Results Reports	70
Issue Reports	70
Generating Issue Reports	72
Legacy Reports	74
Generating Legacy Issue Reports	74
Legacy Report Templates	75
Opening Legacy Report Templates	75
Selecting Legacy Report Sections	75
Editing Legacy Report Subsections	76
Saving Legacy Report Templates	78
Saving Changes to Legacy Report Templates	78
Legacy Report Template XML Files	79
Adding Legacy Report Sections	79
Adding Report Subsections	79
Working with Audit Projects	81
Opening Audit Projects	81
Configuring the Default Filter Set for Auditing	82
About Merging Audit Data	82
Merging Audit Data	83
Performing a Collaborative Audit	83
Uploading Results to Fortify Software Security Center	84
Integrating with a Bug Tracker Application	85
Filing Bugs to Azure DevOps Server	85
Troubleshooting	85
Enabling Debug Mode	86
Locating the Log Files	86
Chapter 3: Remediating Results from Fortify Software Security Center	87
Requirements for Remediating Results	87
Opening a Fortify Software Security Center Application	88

Viewing Analysis Results from Fortify Software Security Center	88
Viewing and Selecting Issues	89
Grouping Issues	91
Customizing Issue Visibility	93
Searching for Issues	94
Search Syntax	94
Search Modifiers	95
Viewing Issue Information	99
Audit Tab	100
Recommendations Tab	101
Details Tab	102
History Tab	102
Locating Issues in Source Code	102
Auditing Analysis Results	103
Auditing Multiple Issues	104
Suppressing Issues	106
Send Documentation Feedback	108

Preface

Contacting Customer Support

Visit the Support website to:

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

<https://www.microfocus.com/support>

For More Information

For more information about Fortify software products:

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

Product feature videos

You can find videos that highlight OpenText Application Security Software products and features on the [Fortify Unplugged YouTube™ channel](#).

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
25.2.0	Updated: Release date and version
24.4.0	Updated: Release date and version
24.2.0	<p>Added:</p> <ul style="list-style-type: none">Remediating analysis results on Fortify Software Security Center:<ul style="list-style-type: none">"Auditing Multiple Issues" on page 104"Suppressing Issues" on page 106 <p>Updated:</p> <ul style="list-style-type: none">Installing Fortify Extension for Visual Studio from the Visual Studio Marketplace (see "Installing Fortify Extension for Visual Studio" on page 11)Ability to perform analysis with Fortify ScanCentral SAST using a standalone ScanCentral SAST client (see "Requirements for Analyzing Source Code" on page 17, "About Scanning with Fortify ScanCentral SAST" on page 28, "Configuring Fortify ScanCentral SAST Options" on page 30, and "Scanning Projects or Solutions with Fortify ScanCentral SAST" on page 32)Added New Issue by Category grouping attribute (see "Grouping Issues" on page 46)
23.2.0	<p>Added:</p> <ul style="list-style-type: none">"Configuring the Default Filter Set for Auditing" on page 82 <p>Updated:</p> <ul style="list-style-type: none">Added that you should save all files in a solution before scanning (see "Scanning Projects or Solutions Locally" on page 28)Added descriptions for the OWASP MASVS 2.0 and the

Software Release / Document Version	Changes
	<p>OWASP API Top 10 reports (see "Issue Reports" on page 70)</p> <ul style="list-style-type: none">• Added a description of the Priority Override grouping attribute (see "Grouping Issues" on page 91)

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:

Product name changes	10
Fortify Extension for Visual Studio	10
Fortify Security Content	11
Installing Fortify Extension for Visual Studio	11
Related documents	12

Product name changes

OpenText is in the process of changing the following product names:

Previous name	New name
Fortify Static Code Analyzer	OpenText™ Static Application Security Testing (OpenText SAST)
Fortify Software Security Center	OpenText™ Application Security
Fortify WebInspect	OpenText™ Dynamic Application Security Testing (OpenText DAST)
Fortify on Demand	OpenText™ Core Application Security
Debricked	OpenText™ Core Software Composition Analysis (OpenText Core SCA)
Fortify Applications and Tools	OpenText™ Application Security Tools

The product names have changed on product splash pages, mastheads, login pages, and other places where the product is identified. The name changes are intended to clarify product functionality and to better align the Fortify Software products with OpenText. In some cases, such as on the documentation title page, the old name might temporarily be included in parenthesis. You can expect to see more changes in future product releases.

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 Opentext™ OpenText SAST and OpenText Secure Coding Rulepacks to locate security vulnerabilities in your solutions and projects (includes support for the following languages: C/C++, C#, Visual Basic (VB.NET), and ASP.NET). The analysis results are displayed in Visual Studio and include a list of issues uncovered, descriptions of the vulnerability type each issue represents, and suggestions on how to fix them.

Your organization can also use the Fortify Extension for Visual Studio with Opentext™ 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

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

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

OpenText provides the ability to write custom rules that add to the functionality of OpenText SAST and the OpenText 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 OpenText Secure Coding Rulepacks. You can also customize the external metadata to map Fortify issues to different taxonomies, such as internal application security standards or additional compliance obligations. For instructions on how to create your own custom rules or custom external metadata, see the *OpenText™ Static Application Security Testing Custom Rules Guide*.

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

Typically, you obtain the current Fortify security content when you install OpenText SAST. For information about updating Fortify security content, see ["Updating Security Content" on page 23](#).

Installing Fortify Extension for Visual Studio

You install the Fortify Extension for Visual Studio either by selecting the extension as a component when you install OpenText Application Security Tools or from the Visual Studio Marketplace.

To install the Fortify Extension for Visual Studio with the OpenText™ Application Security Tools installer, see the *OpenText™ Application Security Tools Guide*. During the OpenText™ Application Security Tools installation, make sure that you select the extension that corresponds to the Visual Studio version installed on your system.

Installing from the Visual Studio Marketplace

To install the Fortify Extension for Visual Studio from the marketplace:

1. In Visual Studio, access the dialog box to manage extensions.
2. Search the Visual Studio Marketplace for Fortify Extension for Visual Studio.
3. Download and install the Fortify Extension for Visual Studio for your version of Visual Studio.

Note: To install this extension as an administrator and allow all users to use the extension, download the VSIX file from the marketplace and then install it using VSIXInstaller with the /admin option from the Command Prompt.

Important! You must also have the OpenText™ Application Security Tools installed and configured in Fortify Extension for Visual Studio. If it is not yet configured, you are prompted to configure the OpenText™ Application Security Tools installation directory when you start Visual Studio. You can also configure the installation directory from the Fortify extension menu in **Options** on the **Apps and Tools Configuration** page.

Related documents

This topic describes documents that provide information about OpenText Application Security Software products.

Note: Most guides are available in both PDF and HTML formats.

All products

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

Document / file name	Description
<i>About OpenText Application Security Software Documentation</i> appsec-docs-n-<version>.pdf	This paper provides information about how to access OpenText Application Security Software product documentation. Note: This document is included only with the product download.

Document / file name	Description
<i>What's New in OpenText Application Security Software <version></i> appsec-wn-<version>.pdf	This document describes the new features in OpenText Application Security Software products.
<i>OpenText Application Security Software Release Notes</i> appsec-rn-<version>.pdf	This document provides an overview of the changes made to OpenText Application Security Software for this release and important information not included elsewhere in the product documentation.

Fortify ScanCentral SAST

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

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

Fortify Software Security Center

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

Document / file name	Description
<i>OpenText™ Application Security User Guide</i> ssc-ugd-<version>.pdf	This document provides Fortify Software Security Center users with detailed information about how to deploy and use Fortify Software Security Center. It provides all the information you need to deploy, configure, and use Fortify Software Security Center.

Document / file name	Description
	It is intended for use by system and instance administrators, database administrators (DBAs), enterprise security leads, development team managers, and developers. Fortify Software Security Center provides security team leads with a high-level overview of the history and status of a project.

OpenText SAST

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

Document / file name	Description
<i>OpenText™ Static Application Security Testing User Guide</i> sast-ugd-<version>.pdf	This document describes how to install and use OpenText SAST to scan code on many of the major programming platforms. It is intended for people responsible for security audits and secure coding.
<i>OpenText™ Static Application Security Testing Custom Rules Guide</i> sast-cr-ugd-<version>.zip	<p>This document provides the information that you need to create custom rules for OpenText SAST. 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>
<i>OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide</i> lim-ugd-<version>.pdf	This document describes how to install, configure, and use the Fortify License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.

OpenText Application Security Tools

The following documents provide information about OpenText Application Security Tools. These documents are available on the Product Documentation website at

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

Document / file name	Description
<i>OpenText™ Application Security Tools Guide</i> sast-tgd-<version>.pdf	This document describes how to install application security tools. It provides an overview of the applications and command-line tools that enable you to scan your code with OpenText SAST, review analysis results, work with analysis results files, and more.
<i>OpenText™ Fortify Audit Workbench User Guide</i> awb-ugd-<version>.pdf	This document describes how to use Fortify Audit Workbench to scan software projects and audit analysis results. This guide also includes how to integrate with bug trackers, produce reports, and perform collaborative auditing.
<i>OpenText™ Fortify Plugin for Eclipse User Guide</i> ep-udg-<version>.pdf	This document provides information about how to install and use the Fortify Plugin for Eclipse to analyze and audit your code.
<i>OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studio User Guide</i> iap-udg-<version>.pdf	This document describes how to install and use the Fortify Analysis Plugin for IntelliJ IDEA and Android Studio to analyze your code and optionally upload the results to Fortify Software Security Center.
<i>OpenText™ Fortify Extension for Visual Studio User Guide</i> vse-ugd-<version>.pdf	This document provides information about how to install and use the Fortify Extension for Visual Studio to analyze, audit, and remediate your code to resolve security-related issues in solutions and projects.

Chapter 2: Using the Fortify Extension for Visual Studio

Use the Fortify Extension for Visual Studio to perform OpenText SAST scans, review and audit analysis results, and remediate issues in Visual Studio.

This section contains the following topics:

About Analyzing the Source Code	16
Working with Fortify Software Security Center	18
About Scanning Locally	21
About Scanning with Fortify ScanCentral SAST	28
Viewing Analysis Results	34
Auditing Analysis Results	57
Using Issue Templates	59
Configuring Custom Tags for Auditing	61
Creating a Filter Set	64
Managing Folders	67
Generating Analysis Results Reports	70
Working with Audit Projects	81
Integrating with a Bug Tracker Application	85
Troubleshooting	85

About Analyzing the Source Code

You analyze the source code from Visual Studio at the solution or project level. A security analysis with OpenText SAST consists of the following main phases:

- Translate all .NET files and other existing supported files, such as T-SQL, into intermediate files
- Scan the intermediate files to complete the security analysis

There are two ways to analyze your source code:

- Use a locally installed OpenText SAST to perform the entire analysis (translation and scan phases). For information about how to configure and run the analysis locally, see ["About Scanning Locally" on page 21](#).

After the scan is complete, Fortify Extension for Visual Studio displays the analysis results in Visual Studio.

- Use OpenText™ Fortify ScanCentral SAST to perform the entire analysis (translation and scan phases) or only the scan phase. For information about how to configure and run the analysis using Fortify ScanCentral SAST, see ["About Scanning with Fortify ScanCentral SAST" on page 28](#).

Note: If you use Fortify ScanCentral SAST to perform only the scan phase, then the Fortify Extension for Visual Studio performs the translation phase using a locally installed OpenText SAST.

After the scan is complete, do one of the following to view the analysis results:

- Configure the Fortify ScanCentral SAST options to upload the analysis results to a Fortify Software Security Center server. You can then open the analysis results from Fortify Extension for Visual Studio (see ["Remediating Results from Fortify Software Security Center" on page 87](#)).
- Use the provided job token in the Fortify ScanCentral SAST client command-line to retrieve the analysis results (FPR) file from the Fortify ScanCentral SAST Controller (see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide* for instructions), and then open it in Visual Studio (see ["Opening Audit Projects" on page 81](#)).

Requirements for Analyzing Source Code

Make sure you meet the following requirements, which depend on how you analyze your code and if you will upload your analysis results to Fortify Software Security Center.

To scan your code from Visual Studio, you must have either:

- A locally installed and licensed OpenText SAST installed with Fortify security content
For installation instructions, see the *OpenText™ Static Application Security Testing User Guide*.
- A local Fortify ScanCentral SAST client and a properly configured Fortify ScanCentral SAST installation

You can install Fortify ScanCentral SAST client, as a component with either the OpenText SAST or the OpenText™ Application Security Tools installation or from a Fortify ScanCentral SAST ZIP archive.

To upload the analysis results to Fortify Software Security Center, you must have the following:

- A Fortify Software Security Center URL
- If your Fortify Software Security Center server uses an SSL connection from an internal certificate authority or a self-signed certificate, you must import the Fortify Software Security Center certificate into the local Windows certificate store.
- A user account on the Fortify Software Security Center server that has permission to access application versions

To log into Fortify Software Security Center, you can use a user name and password, an authentication token, or a single sign-on (SSO) method as configured by a Fortify Software Security Center administrator.

Working with Fortify Software Security Center

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

- Upload your analysis results to Fortify Software Security Center
- Audit applications collaboratively using Fortify Software Security Center
- Update your Fortify security content from Fortify Software Security Center

The following sections describe how to configure a connection to the Fortify Software Security Center server, the different login methods and how to synchronize your work on audit projects with Fortify Software Security Center.

Configuring a Connection to Fortify Software Security Center

Before you can upload to or access the audit results in Fortify Software Security Center, you need to configure your connection to Fortify Software Security Center.

If your Fortify Software Security Center server uses an SSL connection from an internal certificate authority or a self-signed certificate, you must import the Fortify Software Security Center certificate into the local Windows certificate store.

To configure a connection to Fortify Software Security Center:

1. From the Fortify extension menu, select **Options**.
2. In the left pane, select **Server Configuration**.
3. Under **Software Security Center**, specify the **Server URL** for Fortify Software Security Center.

Tip: Click **Test Connection** to confirm that the URL is valid, and you can successfully connect to the Fortify Software Security Center server.

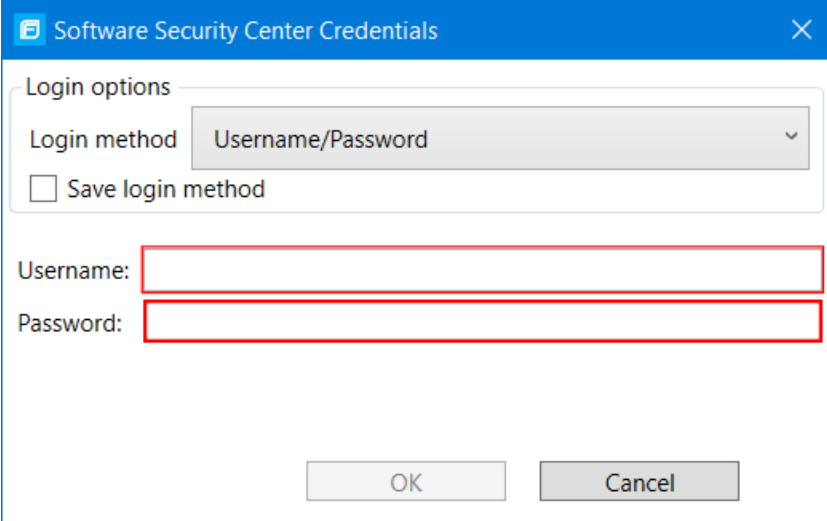
4. Click **OK**.

Logging in to Fortify Software Security Center

The first time you perform an operation that requires a connection to Fortify Software Security Center such as uploading an audit project or opening a collaborative application, you are prompted to log in. Before you can log in, you must have already configured the Fortify Software Security Center URL as described in ["Configuring a Connection to Fortify Software Security Center" above](#).

To log in to Fortify Software Security Center:

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



2. 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.
3. Depending on the login method you selected, do one of the following:

Login Method	Procedure
Username/Password	Type your Fortify Software Security Center user name and password.
Authentication Token	<p>Specify the decoded value of a Fortify Software Security Center authentication token of type ToolsConnectToken.</p> <p>Note: For instructions on how to create an authentication token from Fortify Software Security Center, see the <i>OpenText™ Application Security User Guide</i></p>
X.509 SSO	<p>Fortify Software Security Center must be configured to use X.509 Certification-based SSO.</p> <p>Note: Your certificate must be in the current user certificate store and in the Personal store.</p> <ol style="list-style-type: none">a. Click the Browse for Certificate button .b. Select the certificate for the sign-on, and then click OK.
Kerberos	Fortify Software Security Center must be configured to use SPNEGO-based Kerberos authentication.

Login Method	Procedure
	Note: Support for Kerberos SSO is limited to Windows systems.

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

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 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 later.

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.

If synchronization is enabled, then when you perform a scan, partial scan, save, or merge on your project, a dialog box prompts you to specify whether you want to auto-synchronize your project with the server.

To change whether synchronization occurs automatically with the server:

- From the Fortify extension menu, select **Options**.
- In the left pane, select **Project Configuration**.
- Select the **Synchronization Options** tab.
- Specify the scope of the configuration by doing one of the following:
 - To configure the settings for the projects in the open solution only, select the **Enable Project Specific Settings** check box.
 - To change the default audit configuration for all projects scanned from this Visual Studio instance, click **Configure Defaults**.
- Either clear the **Auto Synchronize all Projects with Server Applications** check box to turn off automatic synchronization or select it to enable automatic synchronization.
- If automatic synchronization is enabled, you can customize the actions that trigger synchronization with the server by selecting the actions to exclude.
- Click **OK**.

About Scanning Locally

This section describes how to perform a scan of your source code on the local system. You must provide the Fortify Extension for Visual Studio with the location of a locally installed OpenText SAST. You are prompted for location of OpenText SAST (sourceanalyzer.exe) the first time you analyze your solution (or project).

In the analysis configuration, you can specify the SQL type, how much memory to use for the scan, select the security content you want to use, whether you want to scan in quick scan mode, and other advanced scanning options.

OpenText strongly recommends that you periodically update the security content, which contains OpenText Secure Coding Rulepacks and external metadata. For information about how to update the security content, see ["Updating Security Content" on page 23](#).

Configuring Security Content Updates

You can configure the server from which to update security content and whether to have the security content updated from a server automatically. To configure these settings, you must provide the location of a locally installed OpenText SAST. You can specify the location of OpenText SAST on the **Security Content Management** options page.

To update security content from your local system (if you do not have an internet connection or a Fortify Software Security Center server), see ["Updating Security Content" on page 23](#).

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

1. From the Fortify extension menu, select **Options**.
The Options dialog box opens to the **Server Configuration** page.

Server Configuration

Security Content Update

☐ Update from Software Security Center

☒ Update from Fortify Update Server

Server URL:

Proxy Server: Port:

Username:

Password:

☐ Update security content automatically

Update Frequency (Days)

Software Security Center

Server URL:

2. To update security content from your Fortify Software Security Center server:
 - a. Under **Security Content Update**, select the **Update from Software Security Center** check box.
 - b. Under **Software Security Center**, specify the **Server URL** for Fortify Software Security Center (for example, `http://my.domain.com:8080/ssc`).
3. To update security content from the Fortify Rulepack update server:
 - a. Under **Security Content Update**, select the **Update from Fortify Update Server** check box.
 - b. In the **Server URL** box, type the URL for the Fortify Rulepack update server.
 - c. If required, specify the proxy server, port number, and credentials for proxy authentication.

Note: When you specify the proxy settings, exclude the protocol from the proxy server (for example, `some.secureproxy.com`). You must specify a proxy port number.
4. To update security content from a server automatically and with a specific frequency:
 - a. Under **Security Content Update**, select the **Update security content automatically** check box.
 - b. In the **Update Frequency (Days)** box, specify how often to update Fortify security content.

See Also

["Updating Security Content" on the next page](#)

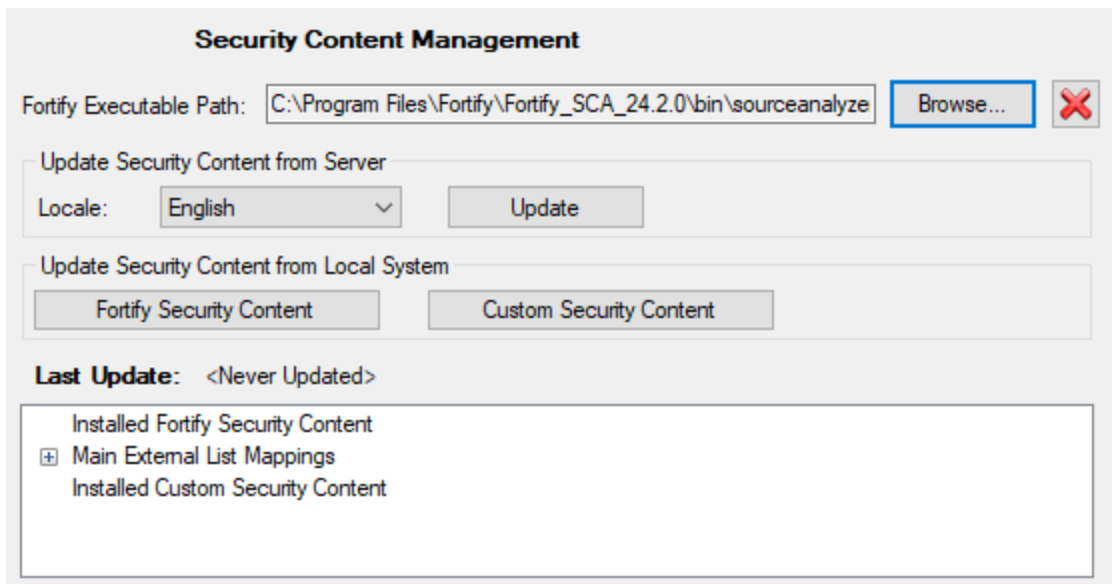
["Importing Custom Security Content" on page 24](#)

Updating Security Content

To enable the Fortify Extension for Visual Studio to scan with a locally installed OpenText SAST, you must have up-to-date security content. You can update Fortify security content from a configured server or from your local system.

To update security content:

1. From the Fortify extension menu, select **Options**.
2. In the left pane, select **Security Content Management**.



3. To update security content, you must provide the location of a locally installed OpenText SAST. If not already specified, do the following:
 - a. Click **Browse** to the right of **Fortify Executable Path**.
 - b. Navigate to the OpenText SAST installation folder.
The default installation folder on Windows is: C:\Program Files\Fortify\Fortify_SCA_<version>.
 - c. Click **OK**.
4. To update Fortify security content from a server, do the following:
 - a. (Optional) From the **Locale** list, select the language you want for the Fortify security content.
By default, English is the selected language.
 - b. Click **Update**.
All existing security content is replaced with the Fortify security content from the server.
5. To update Fortify security content from your local system, under **Update Security Content from Local System**, do the following:
 - a. Click **Fortify Security Content**.
 - b. Navigate to a Fortify security content ZIP file, and then click **Open**.
6. Click **OK** to accept the update confirmation message.

Any existing custom security content is unchanged.

See Also

["Importing Custom Security Content" below](#)

["Configuring Security Content Updates" on page 21](#)

Importing Custom Security Content

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

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

To import custom rules:

1. From the Fortify extension menu, select **Options**.
2. In the left pane, select **Security Content Management**.
3. Under **Update Security Content from Local System**, click **Custom Security Content**.
The Select Security Content dialog box opens.
4. Select the custom rules files to import (*.xml and *.bin), and then click **Open**.

The **Last Update** information box reflects the imported custom security content.

About Quick Scan Mode

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

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

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

You can use quick scan mode for scans that use a locally installed OpenText SAST. Audit quick analysis results just as you audit full analysis results. To perform a quick scan, see ["Configuring Advanced Local Scan Options" on page 26](#).

Configuring Local Scan Options

Use the analysis configuration to customize the security content, specify the SQL type, and specify the amount of memory OpenText SAST uses during a local scan. To configure these settings, you must provide the location of a locally installed OpenText SAST. You can specify the location of OpenText SAST on the **Security Content Management** page.

To configure the analysis options:

1. From the Fortify extension menu, select **Options**.
2. In the left pane, select **Project Configuration**.

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

The screenshot shows the 'Project Configuration' dialog box with the 'Analysis Configuration' tab selected. At the top, there is a checkbox for 'Enable Project Specific Settings' and a link 'Configure Defaults ...'. Below this are three tabs: 'Analysis Configuration', 'Advanced Scan Options', and 'Synchronization Options'. The 'Analysis Configuration' tab contains two sections: 'Scan Configuration' and 'Security Content'. The 'Scan Configuration' section has a 'SQL Type:' dropdown menu and a 'Memory (MB):' text box. The 'Security Content' section has a checkbox 'Use all installed security content' which is checked. Below this is a list titled 'Installed Fortify Security Content:' with eight items, each with a checked checkbox: 'Fortify Secure Coding Rules, Core Preview, ABAP', 'Fortify Secure Coding Rules, Core, .NET', 'Fortify Secure Coding Rules, Core, ABAP', 'Fortify Secure Coding Rules, Core, ActionScript 3.0', 'Fortify Secure Coding Rules, Core, Android', 'Fortify Secure Coding Rules, Core, Annotations', 'Fortify Secure Coding Rules, Core, Apex', and 'Fortify Secure Coding Rules, Core, C/C++'. At the bottom, there is a section titled 'Installed custom security content:' with an empty text box.

3. Specify the scope of the configuration by doing one of the following:
 - To configure the settings for the projects in the open solution only, select the **Enable Project Specific Settings** check box.
 - To change the default scan configuration for all projects scanned from this Visual Studio instance, click **Configure Defaults**.
4. By default, OpenText SAST 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 OpenText SAST about the SQL type that the project uses. OpenText SAST only scans SQL code if it is included in the project.

5. 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.

6. To customize the security content that you want to use, clear the **Use all installed security content** check box, and then select the OpenText Secure Coding Rulepacks and any specific custom security content that you want to use.
7. Click **OK**.

Configuring Advanced Local Scan Options

Use the advanced scan options to activate or deactivate quick scan mode and customize OpenText SAST translation and scan command-line options. To configure these settings, you must provide the location of a locally installed OpenText SAST. You can specify the location of OpenText SAST on the **Security Content Management** page.

To change the advanced translation and scan options:

1. From the Fortify extension menu, select **Options**.
2. In the left pane, select **Project Configuration**.

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

The screenshot shows the 'Project Configuration' dialog box with the 'Advanced Scan Options' tab selected. The 'Enable Project Specific Settings' checkbox is checked. Below the tabs, there is a section for 'Use Additional Static Code Analyzer Options' which is currently unchecked. Under this section, there are input fields for 'Translate:' and 'Scan:'. Below these is a section for 'Local Scan Options' containing a 'Build ID' input field (marked as optional), a checked 'Merge with Previous Scan' checkbox, and an unchecked 'Enable Quick Scan Mode' checkbox. At the bottom, a 'Command-Line Preview' box displays the command: `-machine-output -b Sample.sln -scan -f C:\Users\... \AppData\Local\Fortify\VS17.0-23.2.0\Sample\Scan-Sample.sln.fpr`.

4. Specify the scope of the advanced scan options by doing one of the following:
 - To configure the options for the projects in the open solution only, select **Enable Project Specific Settings**.
 - To change the default scan options for all projects scanned from this Visual Studio instance, click **Configure Defaults**.
5. Select the **Use Additional Static Code Analyzer Options** check box and type OpenText SAST command-line options for either the translation or scan phase.

Note: These options are also included in a Fortify ScanCentral SAST analysis.

For detailed information about the available OpenText SAST options and the proper syntax, see the *OpenText™ Static Application Security Testing User Guide*.

Under **Local Scan Options**, the **Command-Line Preview** box shows the complete OpenText SAST scan command line.

6. (Optional) In the **Build ID** box, type a build ID for the scan.
The default build ID is the name of the project or solution.
7. To deactivate merging the results of the next scan you run with results from the previous scan, clear the **Merge with Previous Scan** check box.

By default, when you rescan a project from Visual Studio, the scan merges results from the previous scan with the results from the new scan. This enables you to see specifically which issues have been fixed and which issues were introduced since the earlier scan.

8. To perform a quick scan, select the **Enable Quick Scan Mode** check box.
For information about quick scans, see ["About Quick Scan Mode" on page 24](#).
9. Click **OK** to save the advanced scan options.

Scanning Projects or Solutions Locally

Before you start the scan, save all files in the solution, and make sure that the active solution configuration is valid for the projects loaded in the solution. If the configuration is invalid, OpenText SAST cannot successfully scan the solution and a message indicating that the configuration is invalid is written to the log file.

Note: OpenText SAST runs scans in a Java Virtual Machine (JVM).

To scan a solution or project on the local system, start the scan in one of the following ways:

- To scan at the solution level, select **Analyze Solution** from the Fortify extension menu.
- To scan at the project level, select a project, and then select **Analyze Project** from the Fortify extension menu.

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

You can now audit the analysis results in Visual Studio. For instructions, see ["Auditing Issues" on page 58](#). If the codebase was audited before, results from the previous audit are automatically integrated with the new analysis results.

By default, the analysis results are stored as an FPR file in the folder that contains the solution or project. To save this file to a different location, select **Save Audit Project As** from the Fortify extension menu.

About Scanning with Fortify ScanCentral SAST

This section describes the requirements to use Fortify ScanCentral SAST to analyze your code and to upload the analysis results to Fortify Software Security Center.

With Fortify Extension for Visual Studio, you can either:

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

You must translate the project or solution locally if it uses a language that Fortify ScanCentral SAST does not support for remote translation. For a list of languages supported with remote translation, see the *OpenText™ Application Security Software System Requirements* document.

Make sure that the Fortify security content version on the local system is the same as the version on the Fortify ScanCentral sensor. OpenText strongly recommends that you periodically update the security content. For information about how to update the security content locally, see

["Updating Security Content" on page 23](#). Use the fortifyupdate utility to update security content on the Fortify ScanCentral SAST sensor (see the *OpenText™ Static Application Security Testing User Guide*).

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

- A local copy of a Fortify ScanCentral SAST client.
For information on how to obtain a Fortify ScanCentral SAST client, see ["Requirements for Analyzing Source Code" on page 17](#).
- A properly configured Fortify ScanCentral SAST installation
Make sure the configuration for your Fortify ScanCentral SAST client is properly authorized with a client authentication token that matches the setting for the Fortify ScanCentral SAST Controller. For more information, see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.
- To connect to Fortify ScanCentral SAST, you need either:
 - A ScanCentral SAST Controller URL

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

- OpenText SAST: `<sca_install_dir>\jre\lib\security\cacerts`
- OpenText™ Application Security Tools: `<tools_install_dir>\jre\lib\security\cacerts`
- Standalone Fortify ScanCentral SAST client: `<java_home_dir>\lib\security\cacerts`

- A Fortify Software Security Center URL and an authentication token of type ToolsConnectToken
To configure the Fortify Software Security Center URL, see ["Configuring a Connection to Fortify Software Security Center" on page 18](#). For instructions about how to create an authentication token, see the *OpenText™ Application Security User Guide*.

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

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

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

- A Fortify Software Security Center authentication token of type ToolsConnectToken
For instructions on how to create an authentication token, see the *OpenText™ Application Security User Guide*.
- An application and application version that exists in Fortify Software Security Center
- Permission to access the application and application version to which you want to upload

See Also

["Configuring Fortify ScanCentral SAST Options" below](#)

["Scanning Projects or Solutions with Fortify ScanCentral SAST" on page 32](#)

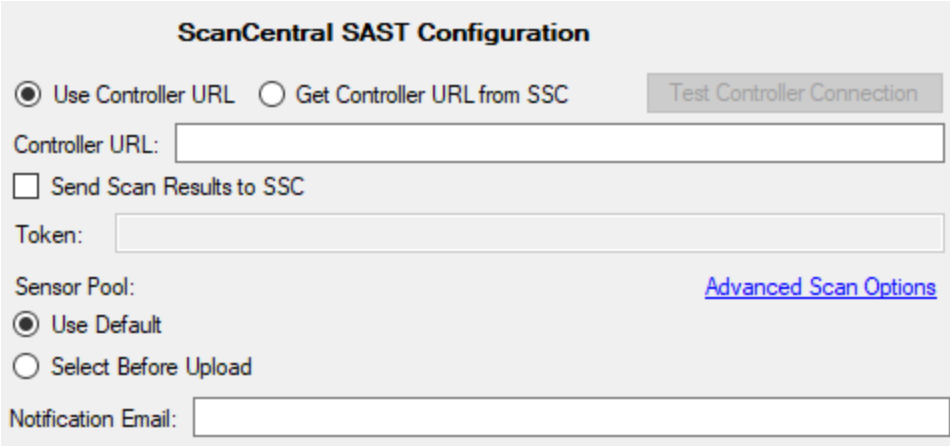
["Advanced Scanning of Solutions with Fortify ScanCentral SAST" on page 33](#)

Configuring Fortify ScanCentral SAST Options

This section describes how to configure the default Fortify ScanCentral SAST options to use when you submit a solution or project for analysis to Fortify ScanCentral SAST. You can specify how to connect to the ScanCentral SAST Controller, the sensor pool selection, and whether to upload analysis results to Fortify Software Security Center. To change the analysis options and perform a scan for a specific solution, see ["Advanced Scanning of Solutions with Fortify ScanCentral SAST" on page 33](#).

To configure the Fortify ScanCentral SAST options:

1. From the Fortify extension menu, select **Options**.
2. To configure the Fortify ScanCentral SAST client location:
 - a. In the left pane, select **Security Content Management**.
 - b. To the right of the **Fortify Executable Path** box, click **Browse**, and do one of the following:
 - If you installed OpenText SAST that includes an embedded Fortify ScanCentral SAST client, select `<scs_install_dir>\bin\sourceanalyzer.exe`.
 - To select a client installed with OpenText™ Application Security Tools, change the file type to **ScanCentral**, and then select `<tools_install_dir>\bin\scancentral.bat`.
 - To select a client installed in a different location, change the file type to **ScanCentral**, and then select `scancentral.bat`.
3. In the left pane, select **ScanCentral SAST Configuration**.



The screenshot shows the "ScanCentral SAST Configuration" dialog box. It has a title bar with the text "ScanCentral SAST Configuration". Inside, there are two radio buttons: "Use Controller URL" (selected) and "Get Controller URL from SSC". To the right of these is a "Test Controller Connection" button. Below the radio buttons is a text box labeled "Controller URL:". There is a checkbox labeled "Send Scan Results to SSC". Below that is a text box labeled "Token:". Underneath is a section for "Sensor Pool:" with two radio buttons: "Use Default" (selected) and "Select Before Upload". To the right of the "Sensor Pool:" section is a link labeled "Advanced Scan Options". At the bottom is a text box labeled "Notification Email:".

4. To specify how to connect to Fortify ScanCentral SAST, do one of the following:
 - Select **Use Controller URL**, and then in the **Controller URL** box, type the URL for the ScanCentral SAST Controller.

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

Tip: Click **Test Controller Connection** to confirm that the URL is valid, and the Controller is accessible.

- Select **Get Controller URL from SSC**, and then in the **Token** box, paste the value for an authentication token of type ToolsConnectToken.

Make sure that you have the Fortify Software Security Center URL that is associated with the ScanCentral SAST Controller provided in the **Server Configuration** options (see ["Configuring a Connection to Fortify Software Security Center" on page 18](#)).

Tip: Click **Test SSC Connection** to confirm that the URL and token is valid, and the server is accessible.

5. To upload the analysis results to Fortify Software Security Center, select the **Send Scan Results to SSC** check box.

- In the **Token** box, paste the value for an authentication token of type ToolsConnectToken.

Note: If you connect to Fortify ScanCentral SAST using a Controller URL, Fortify Extension for Visual Studio uploads analysis results to the Fortify Software Security Center server specifically integrated with the ScanCentral SAST Controller.

6. (Optional) To specify OpenText SAST command-line options for the translation or scan phase:

Important! To specify OpenText SAST command-line options, you must have a local installation of OpenText SAST that includes an embedded Fortify ScanCentral SAST client specified on the **Security Content Management** page.

- a. Click **Advanced Scan Options**.

The **Project Configuration** page opens to the **Advanced Scan Options** tab.

- b. Select the **Use Additional Static Code Analyzer Options** check box and type OpenText SAST command-line options for the translation or scan phase.

For detailed information about the available OpenText SAST options and the proper syntax, see the *OpenText™ Static Application Security Testing User Guide*.

- c. In the left pane, select **ScanCentral SAST Configuration** to return to the Fortify ScanCentral SAST option configuration.

7. Under **Sensor Pool**, specify whether to use the default sensor pool or be provided a list of sensor pools to choose from when you start a scan with Fortify ScanCentral SAST.
8. (Optional) in the **Notification Email** box, type an email address to receive job status notifications.
9. Click **OK** to save your configuration.

Scanning Projects or Solutions with Fortify ScanCentral SAST

Before you can scan your project or solution with Fortify ScanCentral SAST, you must configure the Fortify ScanCentral SAST options as described in ["Configuring Fortify ScanCentral SAST Options" on page 30](#). In addition, make sure that the active solution configuration is valid for the projects loaded in the solution. If the configuration is invalid, OpenText SAST cannot successfully scan the solution and Fortify Extension for Visual Studio writes a message to indicate that the configuration is invalid to the log file.

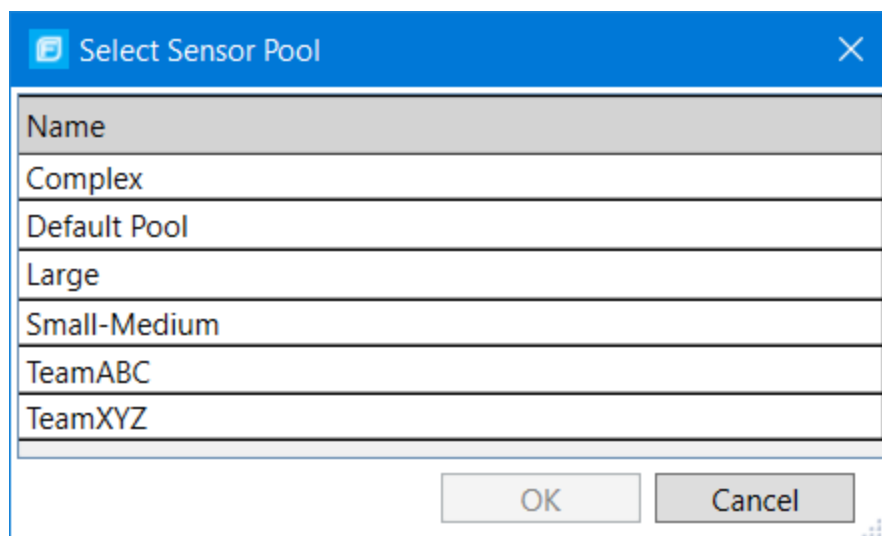
To scan at the solution level with custom Fortify ScanCentral SAST options for this solution, see ["Advanced Scanning of Solutions with Fortify ScanCentral SAST" on the next page](#).

To scan a project or solution with Fortify ScanCentral SAST:

1. Start the scan by doing one of the following:
 - To perform a remote translation and remote scan, select one of the following from the Fortify extension menu:
 - **ScanCentral > Remote > Upload Solution**
 - **ScanCentral > Remote > Upload Project**
 - To perform a local translation and remote scan, select one of the following from the Fortify extension menu:
 - **ScanCentral > Local > Upload Solution**
 - **ScanCentral > Local > Upload Project**

Note: If OpenText SAST is not installed locally, then the **Local** menu command is not available.

2. If prompted, select the application version where you want to upload the analysis results, and then click **OK**.
3. If prompted, select a sensor pool from the Select Sensor Pool dialog box, and then click **OK**.



To view the analysis results, you can either:

- Copy the provided job token and use it in the Fortify ScanCentral SAST client command-line to retrieve the analysis results (FPR) file from the Fortify ScanCentral SAST Controller (see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide* for instructions), and then open it in Visual Studio (see ["Opening Audit Projects" on page 81](#)).
- If you uploaded the analysis results to Fortify Software Security Center, you can check the status of the job (and view the results) on the Fortify Software Security Center server. After the scan is complete, you can open the analysis results in Fortify Extension for Visual Studio (see either ["Performing a Collaborative Audit" on page 83](#) or ["Remediating Results from Fortify Software Security Center" on page 87](#)).

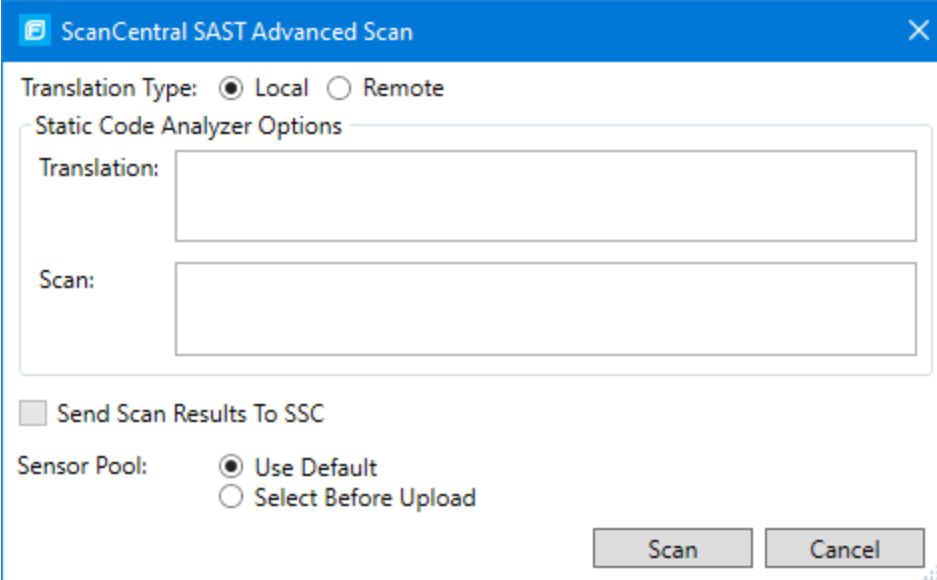
Advanced Scanning of Solutions with Fortify ScanCentral SAST

You can customize the Fortify ScanCentral SAST scan configuration for the current solution. You can adjust the translation type (local or remote), OpenText SAST options for translation and scan, whether to upload analysis results to Fortify Software Security Center, and the sensor pool selection.

To run a customized scan using Fortify ScanCentral SAST:

1. From the Fortify extension menu, select **ScanCentral > Advanced Scan**.

Any existing Fortify ScanCentral SAST configuration options are displayed in the ScanCentral SAST Advanced Scan dialog box.



2. Specify where to run the translation phase of the analysis by selecting one of the following:
 - **Local**—Run the translation phase on the local system and the scan phase with Fortify ScanCentral SAST.
 - **Remote**—Run the entire analysis using Fortify ScanCentral SAST.

3. To specify OpenText SAST command-line options for the translation or scan phase, under **Static Code Analyzer Options**, type command-line options for the translation and scan phase.
For detailed information about the available OpenText SAST options and the proper syntax, see the *OpenText™ Static Application Security Testing User Guide*.

4. To upload the analysis results to Fortify Software Security Center, select the **Send Scan Results to SSC** check box.

Note: If this check box is not available, you must first configure an authentication token in the **ScanCentral SAST Configuration** options (see ["Configuring Fortify ScanCentral SAST Options" on page 30](#)).

5. Specify whether to use the default sensor pool or be prompted to select a sensor pool from a list.
6. Click **Scan**.
7. If prompted, select the application version where you want to upload the analysis results, and then click **OK**.
8. If prompted, select a sensor pool from the Select Sensor Pool dialog box, and then click **OK**.

To view the analysis results, you can either:

- Copy the provided job token and use it in the Fortify ScanCentral SAST client command-line to retrieve the analysis results (FPR) file from the Fortify ScanCentral SAST Controller (see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide* for instructions), and then open it in Visual Studio (see ["Opening Audit Projects" on page 81](#)).
- If you uploaded the analysis results to Fortify Software Security Center, you can check the status of the job (and view the results) on the Fortify Software Security Center server. After the scan is complete, you can open the analysis results in Fortify Extension for Visual Studio (see either ["Performing a Collaborative Audit" on page 83](#) or ["Remediating Results from Fortify Software Security Center" on page 87](#)).

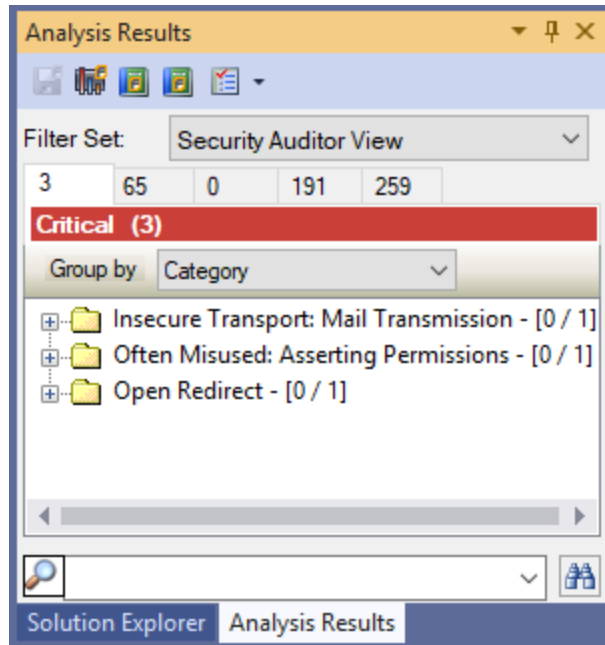
Viewing Analysis Results

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

Window	More Information
Analysis Results	"Analysis Results Window" on the next page
Project Summary	"Viewing Project Summary Information" on page 37
Analysis Trace	"Analysis Trace Window" on page 38
Issue Auditing	"Issue Auditing Window" on page 40

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 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 shows all security issues detected. 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 64](#).

Folders (Tabs)

The tabs on the Analysis Results window are called *folders*. You can customize the settings for the color-coded folders. 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 67](#).

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

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, select a setting from the **Visibility**  list. For more information, see ["Customizing the Issues Display" below](#).

Group By List

The **Group by** selection sorts the issue list into subfolders. The selected attribute is applied to all visible folders. Select **<none>** from the **Group by** list to display all issues in the folder without any grouping. The group by settings are for the application instance. You can apply the grouping attribute 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 grouping.

See Also

["Grouping Issues" on page 91](#)

Customizing the Issues Display

You can customize the issues displayed in the Analysis Results window. Determine which issues it displays by selecting an option from the **Visibility** list  in the **Analysis Results** toolbar.

The visibility options are as follows:

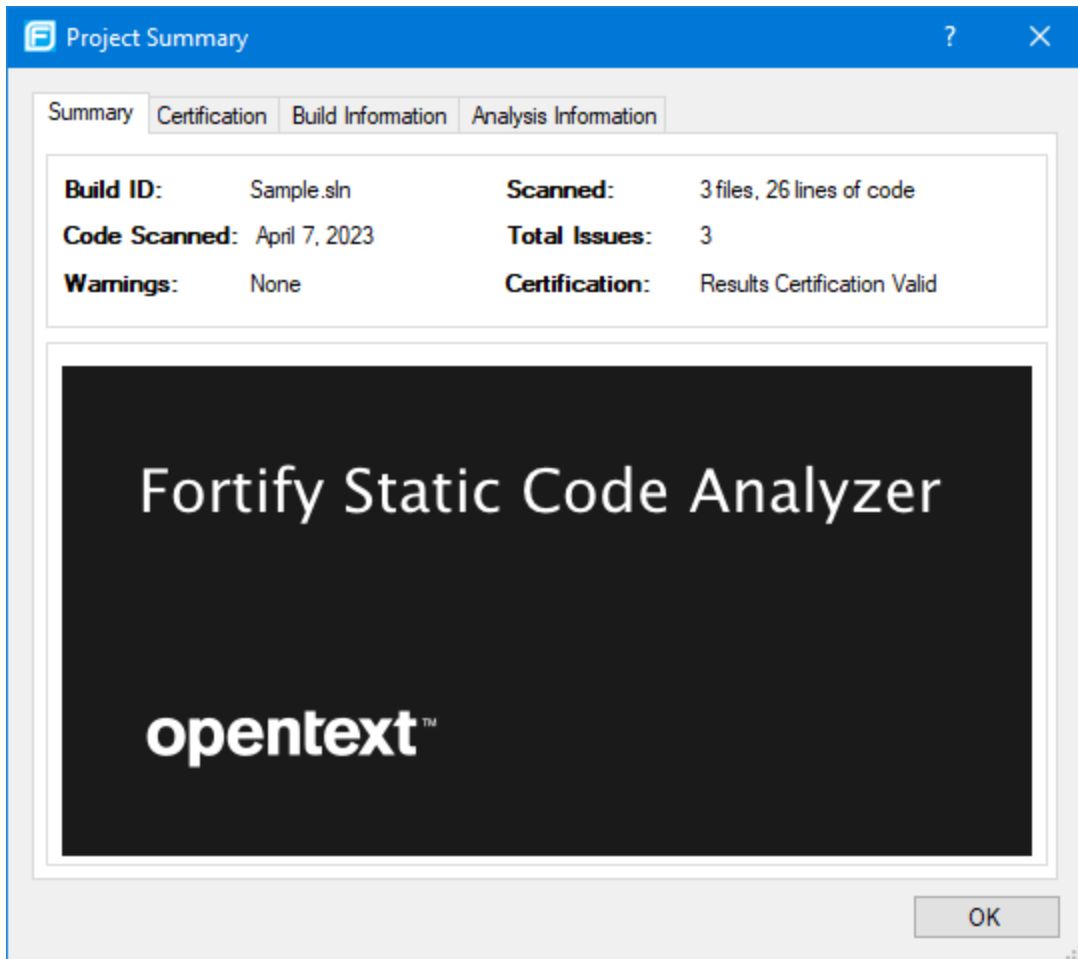
- **Show Removed Issues**—Shows all the issues you have removed or fixed. If you merged audit data into your current audit project, shows all the issues that were removed since the previous analysis.
- **Show Suppressed Issues**—Shows all the issues that you have suppressed.
- **Show Hidden Issues**—Shows all the issues that have been hidden.
- **Show My Issues**—Shows only your issues.
- **Use Short File Name**—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. From the Fortify extension menu, select **Project Summary**.



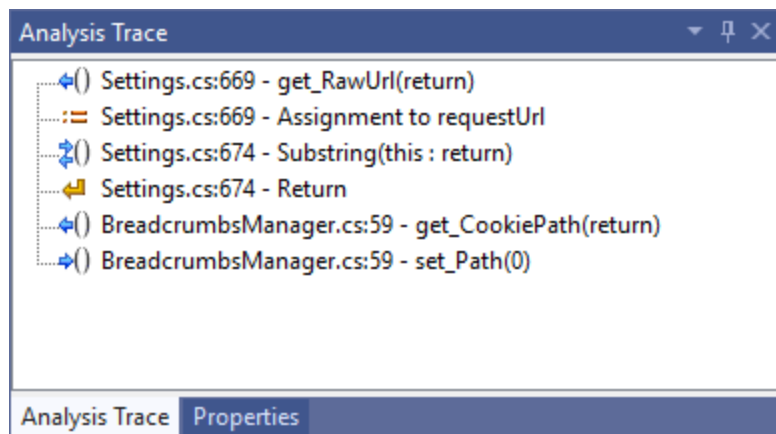
The following table describes the information provided on the Project Summary tabs.

Tab	Description
Summary	Displays high-level audit project information.
Certification	Displays the certification status for the analysis results. Results certification is a check to ensure that the analysis results have not been altered after OpenText SAST produced them.

Tab	Description
Build Information	<p>Displays the following information:</p> <ul style="list-style-type: none">• Build details including the build ID, build label, 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 in the scan
Analysis Information	<p>Displays the version of OpenText SAST that performed the scan, details about the computer on which the scan was run, and the user who started the scan. The Analysis Information subtabs contain the following information:</p> <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 OpenText SAST configuration properties used in the scan• Commandline Arguments—Displays the command-line options used in the scan• Warnings—Lists all errors and warnings that occurred during the scan












Analysis Trace Window










When you select an issue, the Analysis Trace window displays the trace that the analyzer used to detect 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 dataflow, the Analysis Trace window shows the direction of the dataflow in this section of the source code.

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

Icon	Description
	Data is assigned to a field or variable
	Information is read from a source external to the code (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 Note: This is typically shown as <code>functionA(x : y)</code> to indicate that data is transferred from x to y. The x and y values are either: <ul style="list-style-type: none">• An argument index• <code>return</code>—The return value of a function• <code>this</code>—The instance of the current object• A specific object field or key
	An alias is created for a memory location
	Data is read from a variable
	Data is read from a global variable
	Tainted data is returned from a function

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

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

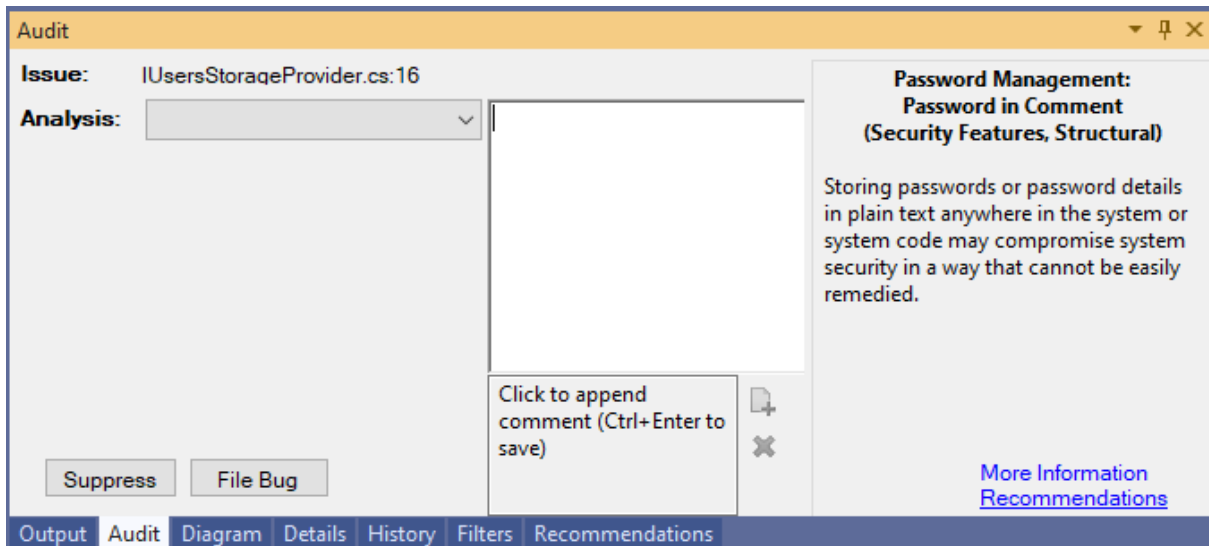
- A text node displayed in italics as a child of the trace node. This text node is expanded by default.
- An induction trace, displayed as a child of the text node.

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



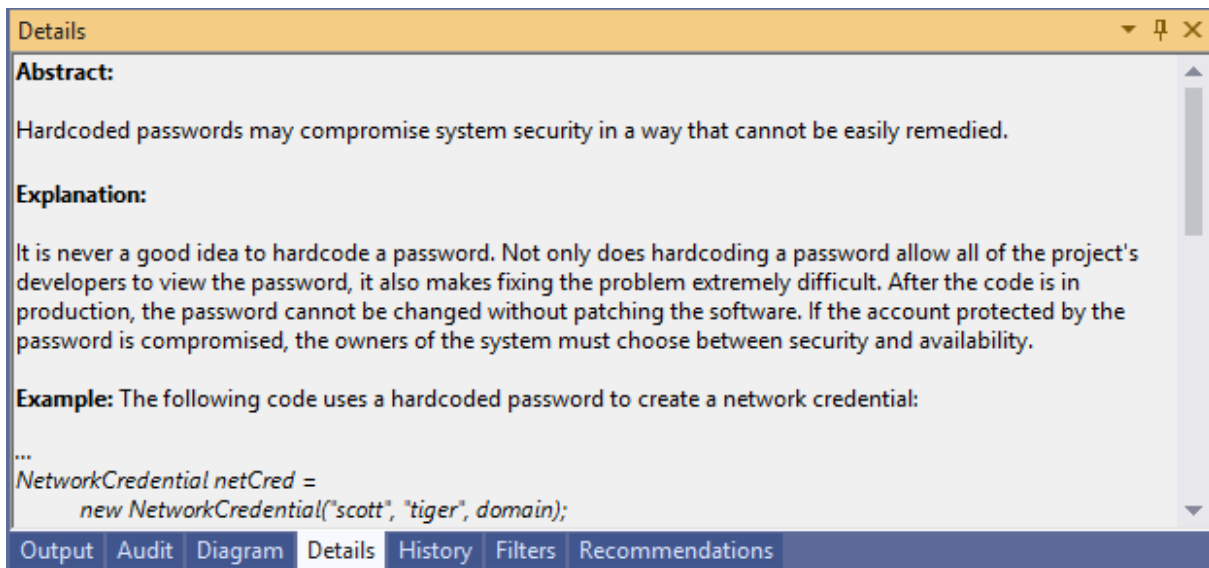
The following table describes the elements of the **Audit** tab.

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 OpenText™ Fortify Audit Assistant in Fortify Software Security Center, then in addition to any other custom tags, the tab displays the following tags:</p> <ul style="list-style-type: none"> • AA_Prediction—Exploitability level that Fortify Audit Assistant assigned to the issue. You cannot change this tag value. • AA_Confidence—Confidence level from Fortify Audit Assistant for the accuracy of its AA_Prediction value. You cannot change this tag value. • AA_Training—Whether to include or exclude the issue from Fortify Audit Assistant training. You can change this value. <p>For more information about Fortify Audit Assistant tags, see the <i>OpenText™ Application Security User Guide</i>.</p>
Suppress	Suppresses the issue.

Element	Description
File Bug	Provides access to a supported bug tracking system, such as Azure DevOps Server. For a list of supported bug tracking systems, see the <i>OpenText™ Application Security Software System Requirements</i> document.
Comments	Submits 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 58](#).

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



The Details tab includes some or all the sections described in the following table.

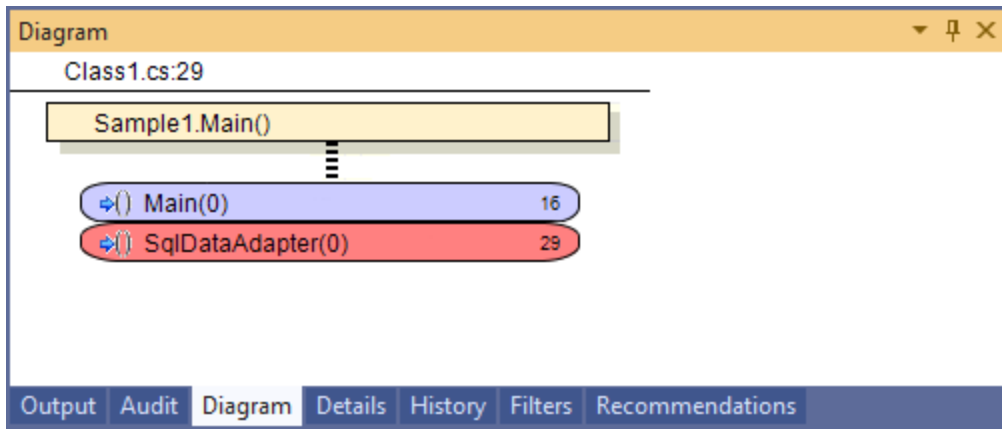
Section	Description
Abstract/Custom Abstract	Summary of the issue, including any custom abstracts defined by your organization.

Section	Description
Explanation/Custom Explanation	Description of the conditions in which this type of issue occurs. This includes a discussion of the vulnerability, the constructs typically associated with it, how an attacker can exploit it, and the potential consequences of an attack. This section also includes any custom explanations defined by your organization.
Instance ID	Unique identifier for the issue.
Primary Rule ID	Identifies the primary rule that found the issue.
Priority Metadata Values	Priority metadata values for this issue including impact and likelihood.
Legacy Priority Metadata Values	Legacy priority metadata values for the issue including severity and confidence.

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

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

- The **History** tab displays 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 displays a graphical representation of the node execution order, call depth, and expression type of the selected issue. This tab displays information that is relevant to the rule type. The vertical axis represents the execution order.

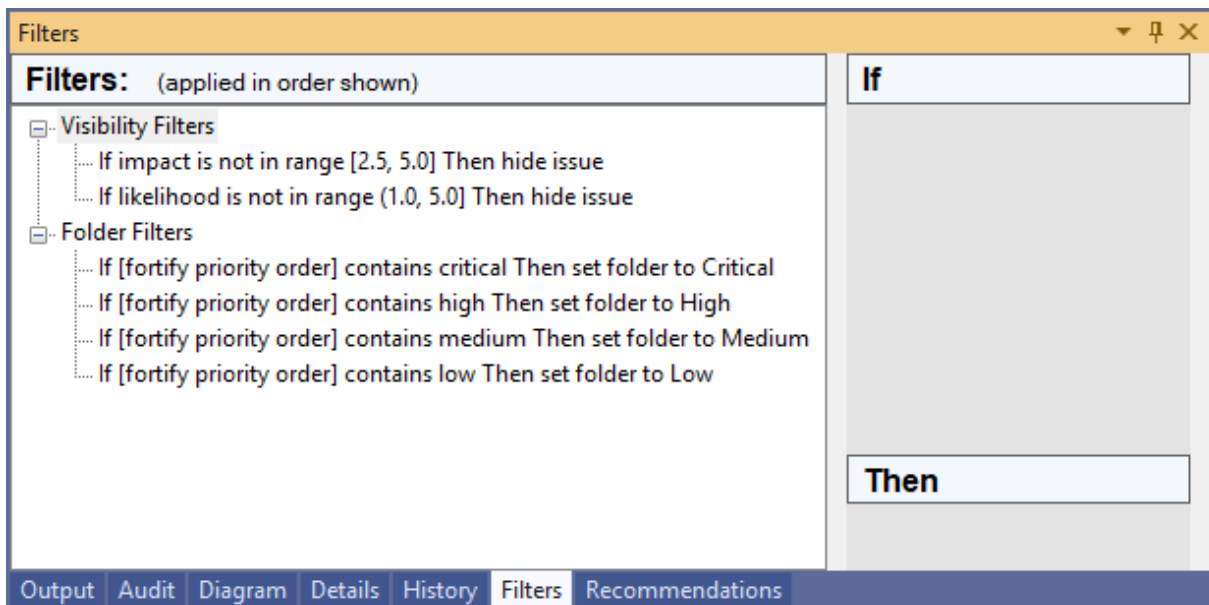


For dataflow issues, the trace starts with the first function to call the taint source, then traces the calls to the source (blue node) and ends the trace at the sink (red node). In the diagram, the source (src) and sink nodes are also labeled. A red X on a vertical axis indicates that the function called 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 Trace window. For a description of the icons, see ["Analysis Trace Window" on page 38](#).

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



The following table describes the options to create new filters.

Option	Description
Filters	<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 is the value the filter matches.</p>
Then	<p>Indicates the filter type, where Hide Issue is a visibility filter and Set Folder to is a folder filter.</p>

For information about creating filters, see ["Creating a Filter from the Filters Tab" on page 65](#).

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 Trace window, the Code Editor shows the code associated with the selected node.

Grouping Issues

The items visible in the Analysis Results window vary depending on the selected grouping attribute. The value you select from the **Group by** list sorts issues in all visible folders into subfolders. The grouping attributes enable you to group and view the issues in different ways.

You can view issues using any of the grouping attributes, and you can create and edit customized groups. The following table describes the standard grouping attributes.

Attribute	Description
Analysis	Groups issues by the analysis tag value assigned, such as Suspicious, Exploitable, and Not an Issue.
Analysis Type	Groups issues by analyzer product, such as SCA, WEBINSPECT, and SECURITYSCOPE (OpenText™ Dynamic Application Security Testing).
Analyzer	Groups issues by analyzer group, such as Control Flow, Data Flow, Semantic, and Structural.
App Defender Protected	Groups issues by whether Application Defender can protect the vulnerability category.
Category	Groups issues by vulnerability category. This is the default setting.
Category Analyzer	Groups issues by category and then by analyzer.
<custom_tagname>	Groups issues by selected custom tag.
File Name	Groups issues by file name.
Fortify Priority Order	Groups issues as Critical, High, Medium, and Low based on the combined values of OpenText SAST impact and likelihood.
Kingdom	Groups issues by the Seven Pernicious Kingdoms classification.
<metadata_listname>	Groups issues using the alternative metadata external list names (for example, OWASP Top 10 <year>, CWE, PCI SSF <version>, STIG <version>, and so on).
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 Issue subfolder and the others are displayed in the Existing Issue subfolder. Issues not found in the latest scan are displayed in

Attribute	Description
	<p>the Removed subfolder.</p> <p>Note: If you are remediating results that reside in Fortify Software Security Center, these subfolders are named NEW, UPDATED, and REMOVED, respectively.</p>
New Issue by Category	Groups issues that are new since the last scan and then by category. Also see "New Issue" on the previous page .
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	Groups issues by Fortify Priority Order and then by category.
Sink	Groups issues that share the same dataflow sink functions.
Source	Groups issues that share the same dataflow source functions.
Taint Flag	Groups issues by the taint flags that they contain.
<none>	Displays a flat view without any grouping.

See Also

["Creating a Custom Group By Option" below](#)

Creating a Custom Group By Option

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

To create a new Group By option:

- From the **Group by** list, select **<Edit>**.
The Edit Custom Groupings dialog box opens.
- 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

In the Analysis Results window, use the search box located below the issue list 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 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 that you used previously (during the current session), click the arrow in the search box, and then select a search term from the list. Fortify Extension for Visual Studio discards saved search terms after you exit Visual Studio.

The Analysis Results window displays the search results.

See Also

["Performing Advanced Searches" below](#)

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

["Search Modifiers" on page 50](#)


["Search Query Examples" on page 55](#)

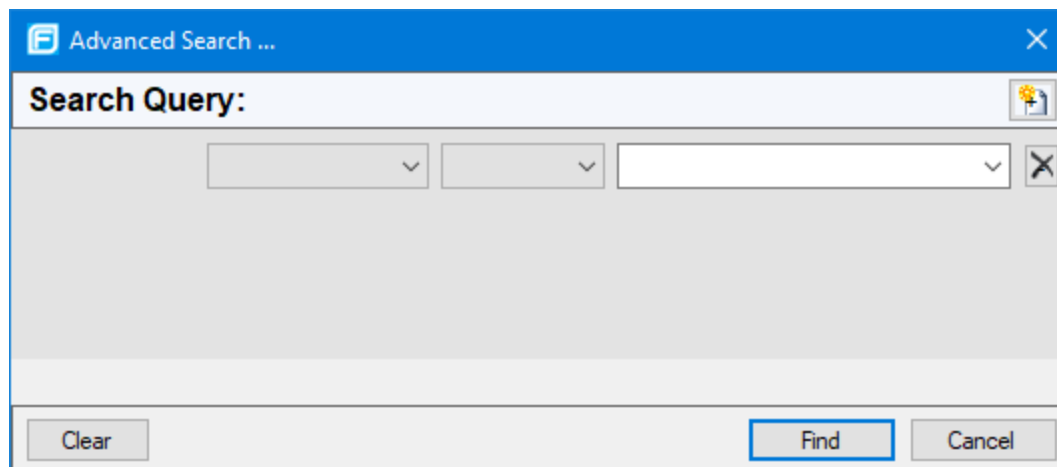
Performing Advanced Searches



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 in Fortify Software Security Center.

To use the advanced search feature:

1. To the right of the search box, click the **Advanced Search** button .
The Advanced Search dialog box opens.



2. From the first list on the left, select a modifier.
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 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 modifier. However, you can type any value into this box.
5. To add an AND or OR row to the query, click the **Add Criteria** button .
6. To set the operator, click either **AND** or **OR**.
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 the **Delete** button .
10. To remove all rows, at the bottom of the dialog box, click **Clear**.
11. To submit your completed search query, click **Find**.

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

Search Syntax

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 (" ")

Comparison	Description
regex	<p>Searches for values that match a Java-style regular expression delimited by a forward slash (/)</p> <p>Example, /eas.+?/</p> <p>Note: This search comparison is not available when you remediate audit results stored in Fortify Software Security Center.</p>
number range	<p>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.</p> <p>Example: (2,4] indicates greater than two and less than or equal to four</p>
not equals	<p>Excludes issues specified by the string by preceding the string with an exclamation character (!)</p> <p>Example, file:!Main.java returns all issues that are not in Main.java.</p>

You can further qualify search terms with modifiers. The syntax for using a modifier is `<modifier>:<search_term>`. For more information, see ["Search Modifiers" below](#).

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. 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.

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

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

The following table 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.

Search Modifier (Issue Attribute)	Description
accuracy	Searches for issues based on the accuracy value specified (0.1 through 5.0).
analysis	Searches for issues that have the specified audit analysis value such as <code>exploitable</code> , <code>not an issue</code> , and so on.
[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 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. Note: This metadata is legacy information that is no longer used and will be removed in a future release. OpenText recommends that you do not use this search modifier.
audited	Searches the issues to find <code>true</code> if the primary tag is set and <code>false</code> if the primary tag is not set. The default primary tag is the Analysis tag.
category (cat)	Searches for the given category or category substring.
class	Searches for issues based on the specified class name.

Search Modifier (Issue Attribute)	Description
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. OpenText SAST calculates the confidence value based on the number of assumptions made in code analysis. The more assumptions made, the lower the confidence value.
<custom_tagname>	<p>Searches for issues based on the value of the specified custom tag.</p> <p>You can search a list-type custom tag using a range of values. The values of a list-type custom tag are an enumerated list where the first value is 0, the second is 1, and so on. You can use the search syntax for a range of numbers to search for ranges of list-type custom tag values. For example, <code>analysis:[0,2]</code> returns the issues that have the values of the first three Analysis values, 0, 1, and 2 (Not an Issue, Reliability Issue, and Bad Practice).</p> <p>To search for a specific date in a date-type custom tag, specify the date in the format: <code>yyyy-mm-dd</code>.</p> <p>To search for issues that have no value set for a custom tag, use <code><none></code> as the search term. For example, to search for all issues that have no value set in the custom tag labeled Target Date, type: <code>[Target Date]:<none></code>.</p>
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 path.
[fortify priority order]	Searches for issues that have a priority level that matches the specified issue priority. Valid values are <code>critical</code> , <code>high</code> , <code>medium</code> , and <code>low</code> .
historyuser	Searches for issues that have audit data modified by the

Search Modifier (Issue Attribute)	Description
	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 new, updated, reintroduced, or removed.
[issue state]	Searches for audited issues based on whether the issue is an open issue or not an issue (determined by the level of analysis set for the primary tag).
kingdom	Searches for all issues in the specified kingdom.
likelihood	Searches for issues based on the specified likelihood value (0.1 through 5.0).
line	Searches for issues on the primary location line number. For dataflow issues, the value is the sink line number. Also see "sourceline" on 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.
<metadata_listname>	Searches for issues based on the value of the specified metadata external list. Metadata external lists include [owasp top ten <year>], [cwe top 25 <version>], [pci ssf <version>], [stig <version>], and others.
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

Search Modifier (Issue Attribute)	Description
	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	Searches for all issues reported by the specified rule IDs used to generate the issue source, sink, and all passthroughs.
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 dataflow issues with the source function call that the specified file contains. Also see " file " on page 52.
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.

Search Modifier (Issue Attribute)	Description
trace	Searches for issues that have the specified string in the dataflow trace.
tracenode	Enables you to search on the nodes within an issue's analysis trace. Each tracenode search value is a concatenation of the tracenode's file path, line number, and additional information.
tracenodeallpaths	Searches for the specified value in all the steps of the analysis trace.
url	Searches for issues based on the specified URL.
user	Searches for issues assigned to the specified user.

Search Query Examples

The following table contains search query examples.

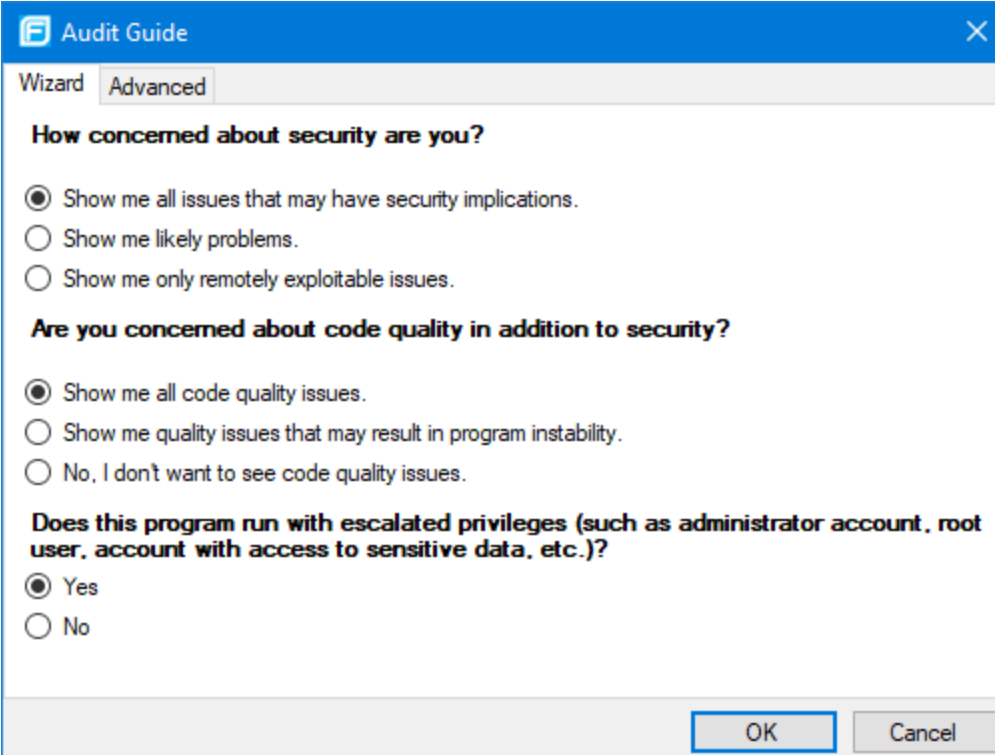
Search Target	Query
All privacy violations in file names that contain jsp with getSSN() as a source	category:privacy_violation source:getssn file:jsp
All file names that contain com/test/123	file:com/test/123
All paths that contain traces with mydbcode.sqlcleanse as part of the name	trace:mydbcode.sqlcleanse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

Filtering Issues with the Audit Guide

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

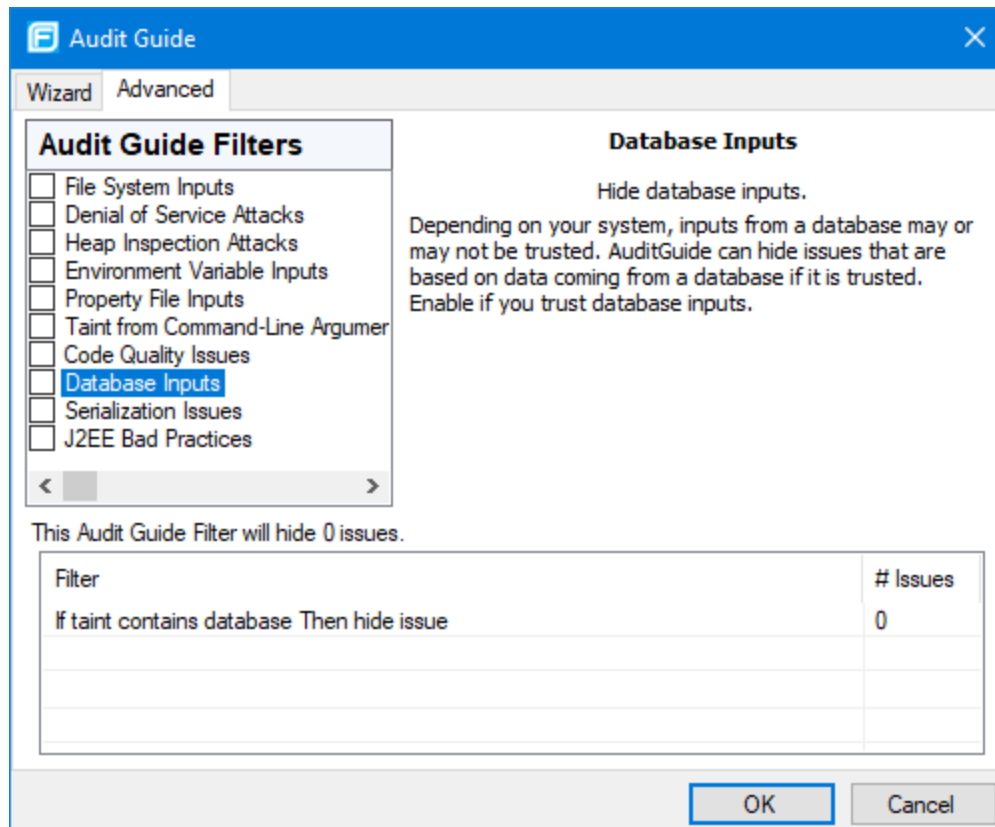
To use the Audit Guide:

1. From the Fortify extension menu, select **Audit Guide**.

The image shows a Windows-style dialog box titled "Audit Guide" with a close button (X) in the top right corner. Inside the dialog, there are two tabs: "Wizard" (which is selected) and "Advanced". The "Wizard" tab contains three sections of questions, each with radio button options. The first section is "How concerned about security are you?" with three options: "Show me all issues that may have security implications." (selected), "Show me likely problems.", and "Show me only remotely exploitable issues.". The second section is "Are you concerned about code quality in addition to security?" with three options: "Show me all code quality issues." (selected), "Show me quality issues that may result in program instability.", and "No, I don't want to see code quality issues.". The third section is "Does this program run with escalated privileges (such as administrator account, root user, account with access to sensitive data, etc.)?" with two options: "Yes" (selected) and "No". At the bottom right of the dialog are "OK" and "Cancel" buttons.

2. Select the settings for the types of issues you want to display.

3. To use the advanced filtering options, select the **Advanced** tab.



- In the **Audit Guide Filters** list, select the types of issues to filter out and ignore.
To see a description on the right side, click an issue type.
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 filter selections.

Auditing Analysis Results

The security team examines the 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.

By default, 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 change 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 might 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 61](#).

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 (see ["Analysis Results Window" on page 35](#)).


Note: If multiple issues are selected, then this information is displayed on the **Audit** tab as **Issue: Multiple Issues Selected**.

2. Read the abstract on the **Audit** tab, which provides high-level information about the issue, such as the analyzer that found the issue.

For example, **Command Injection (Input Validation and Representation, data flow)** indicates that this issue, detected by the Dataflow Analyzer, is a Command Injection issue in the Input Validation and Representation kingdom.

3. Click the **Details** tab to see more details about the issue.
4. On the **Audit** tab, select an analysis value for the issue to represent your evaluation.
5. Specify values for any custom tags as required by your organization.

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

To specify text in a text-type custom tag, click the **Edit Text** button , and then enter text in the Edit Text Value dialog box.

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

Note: If you select a different value for the analysis tag than the **AA_Prediction** value set by Fortify Audit Assistant, and you select Include from the **AA_Training** list, then the next time the data is submitted to Fortify Audit Assistant, it updates the information used to predict whether an issue represents a true vulnerability. For more information about Fortify Audit Assistant tags, see the *OpenText™ Application Security User Guide*.

7. (Optional) In the **Comments** box, click to add comments relevant to the issue and your evaluation, and then click the **Add Comment** button .

Suppressing Issues

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

To suppress an issue, do one of the following:

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

To display results that have been suppressed:

- From the **Visibility** list  list on the **Analysis Results** toolbar, select **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. For a list of supported client-side bug tracking plugins, see the *OpenText™ Application Security Software System Requirements* document.

To submit an issue as a bug:

1. In the Analysis Results window, select an issue.
2. In the Issue Auditing window, select the **Audit** tab, and then click **File Bug**.
If this is the first time you are submitting a bug, the Select Bug Tracker Integration dialog box opens. Select a bug tracking application, and then click **Select**.
3. If prompted, provide your bug tracker login credentials.
4. 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.
5. Click **File Bug**.

The issue is submitted as a bug in the bug tracking application.

Using Issue Templates

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

In addition to providing sorting and filtering mechanisms, you can also customize the auditing process by defining custom tags in the issue template. Auditors associate custom tags with issues during 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. For more information about custom tags, see ["Configuring Custom Tags for Auditing" on the next page](#).

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 tags 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 `<tools_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. From the Fortify extension menu, select **Project Configuration**.
2. Select 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. From the Fortify extension menu, select **Project Configuration**.
2. Select the **Filter Sets** tab.
3. Click **Import Issue Template**.
4. Select the issue template file to import, and then click **Open**.

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 might create a list-type custom tag to track the sign-off process for an issue. After a developer audits his own issues, a security expert can review those same issues and mark each as “approved” or “not approved.”

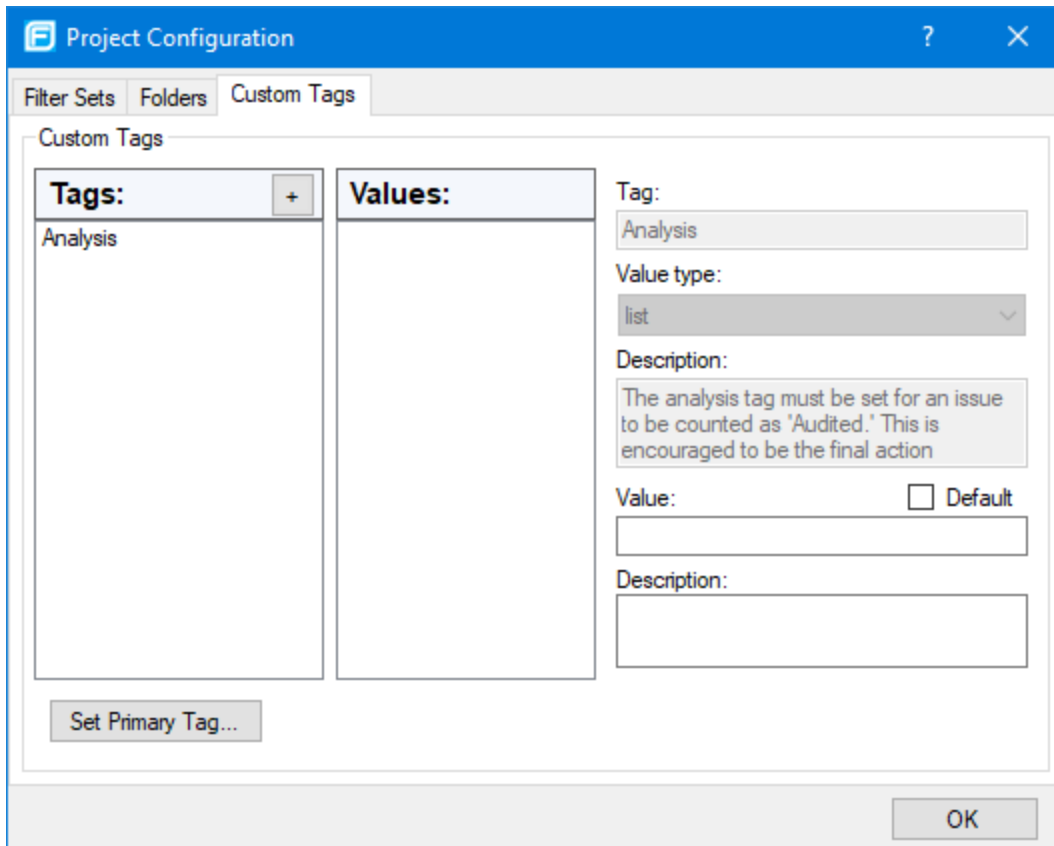
After you define a custom tag, the **Audit** tab displays it below the Analysis tag, which enables you to specify values as they relate to specific issues. The tag is also available in other areas of the interface, such as in the **Group By** list as a way to group issues in a folder, in the search box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


Adding a Custom Tag

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

To add a custom tag:


1. From the Fortify extension menu, select **Project Configuration**.
2. Select the **Custom Tags** tab.



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

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

4. In the Create New Tag 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 the **Add Value** button .
 - 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.
 9. To make this custom tag the primary tag:

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

- a. Click **Set Primary Tag**.
- b. In the Set Primary Tag dialog box, select the custom tag from the **Primary Tag** list, and then click **OK**.


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

Hiding a Custom Tag

If you hide a custom tag, it is no longer available on the **Audit** tab or as a search or filter option. If you hide a custom tag that was set for any issues, that tag and values are hidden from the issue. You can make this tag available again when you create a custom tag (see ["Adding a Custom Tag" on the previous page](#)). If you make the tag available again, the tag and values are restored.

Note: You cannot hide a custom tag that is set as the primary tag.

To hide a custom tag:

1. From the Fortify extension menu, select **Project Configuration**.
2. Select the **Custom Tags** tab.
3. Select the tag from the **Tags** list.
4. Next to **Tags**, click the **Hide Tag** button .

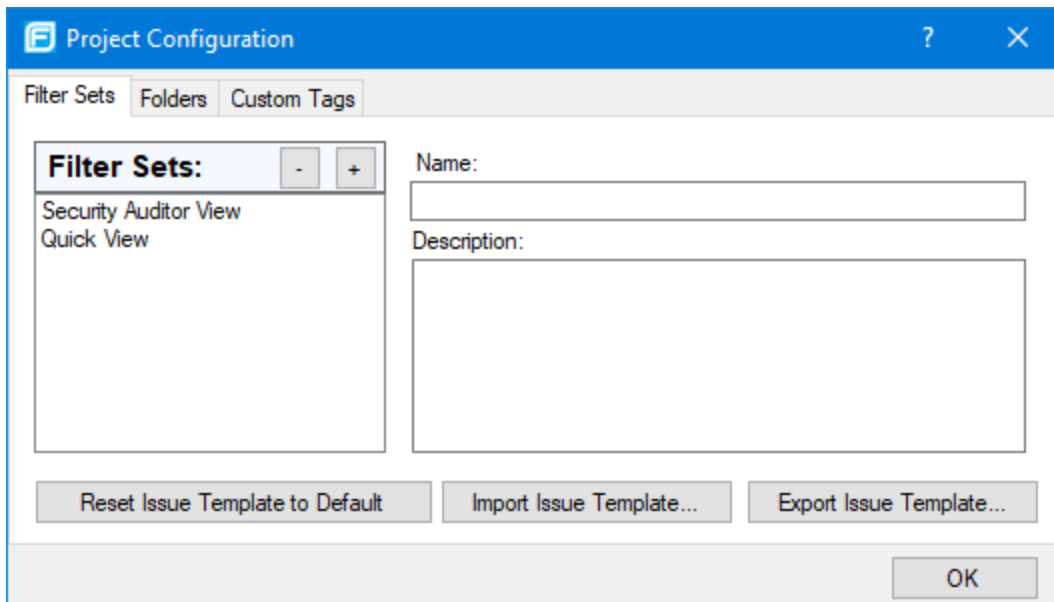
If you hide a tag that has an associated filter, you are prompted to delete the filter.


Creating a Filter Set

To create a new filter set, you copy an existing set, and then make changes the settings.

To create a new filter set:

1. From the Fortify extension menu, select **Project Configuration**.
2. Select the **Filter Sets** tab.



3. Next to **Filter Sets**, click the **Create Filter Set** button .
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.

See Also

["Creating a Filter from the Analysis Results Window" on the next page](#)

["Creating a Filter from the Filters Tab" on the next page](#)

["Copying a Filter to Another Filter Set" on page 66](#)

["Managing Folders" on page 67](#)

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**.
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 for 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.

See Also

["Creating a Filter from the Filters Tab" below](#)

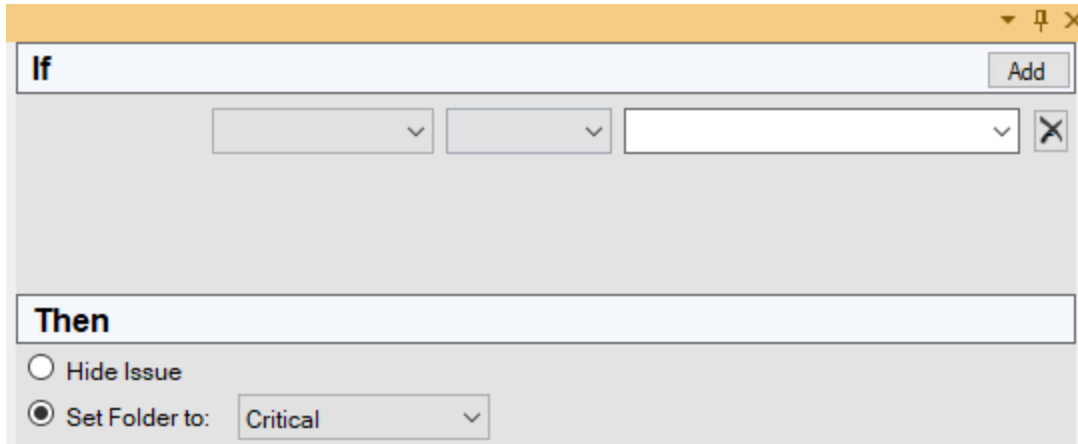
Creating a Filter from the Filters Tab

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. In the Analysis Results window, select a filter set from the **Filter Set** list.
2. In the Filters window, right-click **Visibility Filters** or **Folder Filters**, and then select **Create New Filter**.



3. Under **If**, specify the conditions for the filter, by doing the following:
 - a. From the first list, select an issue attribute.
For a description of the available issue attributes, see ["Search Modifiers" on page 50](#).
 - b. From the second list, select how to match the value.
The third list automatically displays the attribute values.
 - c. From the third list, select a value or specify a range as instructed.
4. 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 is displayed at the end of the list. For folder filters, this gives the new filter the highest priority. Issues that match the new folder filter are displayed in the targeted folder.

5. (Optional) For folder filters, drag the filter higher in the folder filter list to change its priority.

The issues are sorted based on the new filter.

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

See Also

["Creating a Filter from the Analysis Results Window" on the previous page](#)

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. In the Analysis Results window, select a filter set from the **Filter Set** list.
2. On the **Filters** tab, right-click a filter, and then select **Copy Filter To**.
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 the filters in the list.

Managing Folders

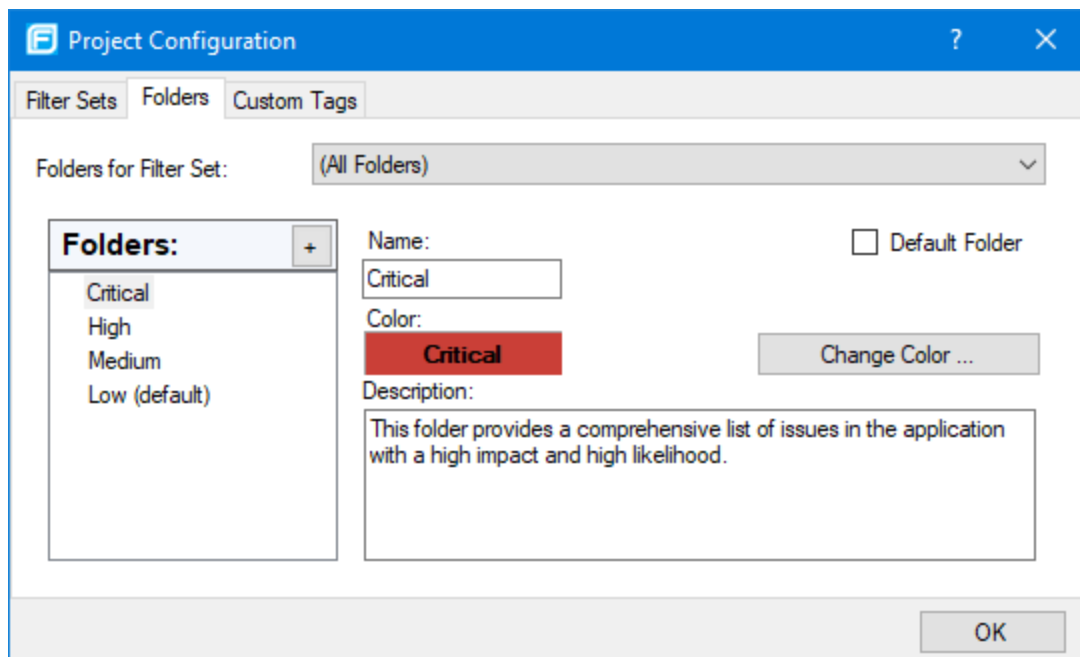
Folders are logical sets of issues that are defined by the filters in the active filter set. Even though a folder can appear in more than one filter set, the contents might differ depending on the filters in that filter set that target the folder. To accommodate filter sets that attempt to provide sorting 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. From the Fortify extension menu, select **Project Configuration**.
2. Select the **Folders** tab.
Currently defined folders are listed on the left. Folder properties including the name, color, and description of the selected folder are shown 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 the **Create Folder** button .

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 the **Default Folder** check box.
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 65](#) and ["Creating a Filter from the Filters Tab" on page 65](#)).

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. From the Fortify extension menu, select **Project Configuration**.
2. Select 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 **Add Folder** button .
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. From the Fortify extension menu, select **Project Configuration**.
2. Select the **Folders** tab.
3. From the **Folders for Filter Set** list, select a filter set that displays the folder you want to rename.
4. In the **Folders** list, select the folder you want to rename.
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 specific filter set without removing it from other filter sets.

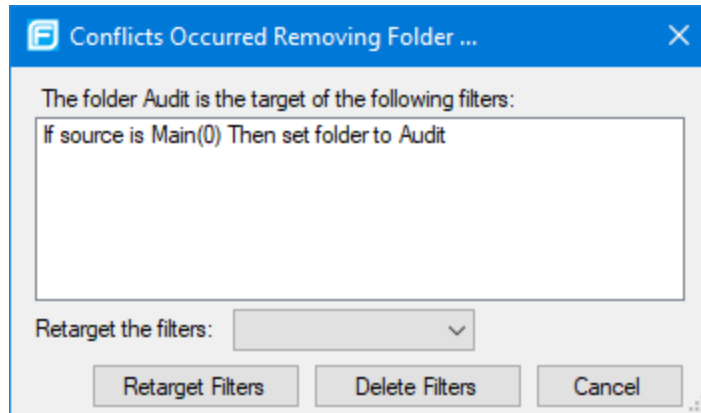
To remove a folder:

1. From the Fortify extension menu, select **Project Configuration**.
2. Select the **Folders** tab.
3. From the **Folders for Filter Set** list, select a filter set, other than **(All Folders)**, that contains the folder you want to remove.
The folders in the selected filter set are listed.
4. In the **Folders** list, select the folder you want to remove.

5. To the right of **Folders**, click the **Remove Folder** button .

The folder is only removed 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.

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

The folder is no longer displayed as a tab in the Analysis Results window.

Generating Analysis Results Reports

The following topics provide information about generating reports from your analysis results.

Issue Reports

The issue reports described in this section are based on the Business Intelligence and Reporting Technology (BIRT) system. You can generate issue reports from the Fortify Extension for Visual Studio or from the command line (BIRTReportGenerator utility). For information about how to generate issue reports based on BIRT from the command line, see the *OpenText™ Static Application Security Testing User Guide*.

The following table describes the issue reports available.

Report Template	Description
CWE Top 25	This report lists the most widespread and critical weaknesses that can lead to serious software vulnerabilities (based on the National Vulnerability Database).

Report Template	Description
CWE/SANS Top 25	This report details issues related to the CWE/SANS Top 25 Most Dangerous Programming Errors and provides information about where and how to fix the issues. It describes the technical risk posed by unremediated issues discovered during analysis and provides an estimate of the development effort needed to test, verify, and fix them.
Developer Workbook	This report provides the information a developer needs to understand and fix the issues discovered during an application audit.
DISA CCI 2	This report provides a standard identifier for policy-based requirements that connects high-level policy expressions and low-level technical implementations.
DISA STIG	This report addresses DISA compliance based on STIG violations and provides information about where and how to fix the issues. It describes the technical risk posed by unremediated issues and provides an estimate of the development effort required to test, verify, and fix them.
FISMA Compliance: FIPS 200	This report addresses FISMA compliance related to FIPS-200 through controls specified in NIST SP 800-53. It details policy violations and provides information about where and how to fix the issues. It describes the technical risks posed by unremediated violations and provides an estimate of the development effort required to test, verify, and fix them.
GDPR	This report groups all detected issues that are relevant to privacy under the EU General Data Protection Regulation (GDPR) legislation. Use this as a framework to help identify and protect personal data as it relates to application security.
MISRA	This report addresses compliance with either the Motor Industry Software Reliability Association (MISRA) C or C++ guidelines. The results focus on the security relevant guidelines and can be used to help create a compliance matrix for MISRA. This report describes the technical risk posed by the unremediated issues discovered during analysis and provides an estimate of the development effort needed to test, verify, and fix them.
OWASP API Top 10	This report focuses on weaknesses affecting Web APIs and is intended to be used in combination with other standards and best practices to thoroughly capture all relevant risks. For example, use this report in combination with the OWASP Top 10 to identify issues related to input

Report Template	Description
	validation such as injections.
OWASP ASVS 4.0	This report groups detected issues based the OWASP Application Security Verification Standard security requirements for secure development.
OWASP MASVS 2.0	This report groups detected issues based on the OWASP Mobile Application Security Verification Standard requirements for secure mobile application development.
OWASP Mobile Top 10	This report details the top ten OWASP mobile-related issues and provides information about where and how to fix them. It describes the technical risk posed by the unremediated issues discovered during analysis and gives an estimate of the development effort required to test, verify, and fix them.
OWASP Top 10	This report details the top ten OWASP-related issues and provides information about where and how to fix them. It describes the technical risks posed by unremediated issues discovered during analysis and gives an estimate of the development effort required to test, verify, and fix the issues.
PCI DSS Compliance: Application Security Requirements	This report summarizes the application security portions of PCI DSS. It includes tests for 21 application security-related requirements across sections 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is either “In Place” or “Not In Place.”
PCI SSF Compliance: Secure Software Requirements	This report summarizes the application security portions of PCI SSF. It includes tests for 23 application security-related control objectives across Control Objective sections 2, 3, 4, 5, 6, 7,8, and A.2 of PCI SSF and reports whether each control objective is "In Place" or "Not In Place."

Generating Issue Reports

To generate an issue report:

1. From the Fortify extension menu, select **Generate BIRT Report**.
The Generate BIRT Report dialog box opens.

Generate BIRT Report

BIRT Report

Report Template:
PCI DSS Compliance: Application Security Requirements

Options: PCI 3.2.1

PCI DSS Compliance

☐ Detailed Report
Provide detailed descriptions of reported issues

☐ Key Terminology
Include the 'Description of Key Terminology' section

☐ About Fortify Solutions
Include the 'About Fortify Solutions' section

Issue Filter Settings

☐ Removed ☐ Suppressed ☐ Hidden

☒ Collapse Issues ☐ Only My Issues

Filter: [Advanced...](#)

Format: PDF

Location: C:\MyReports\ProjectA\Sample PCI DSS Compliance Ap [Browse...](#)

[Generate](#) [Cancel](#)

2. From the **Report Template** list, select the type of report you want.
3. If available for the template, select the template version from the **Options** list.
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:
 - To include removed issues in the report, select the **Removed** check box.
 - To include suppressed issues in the report, select the **Suppressed** check box.

- To include hidden issues in the report, select the **Hidden** check box.
 - To collapse issues of the same sink and type into a single issue, select the **Collapse Issues** check box.
 - To include only issues assigned to your user name, select the **Only My Issues** check box.
 - To build a search query to further filter the issues to include in the report, click **Advanced**. Your query will appear in the **Filter** box. For more information about the search modifiers, see ["Search Modifiers" on page 50](#).
6. From the **Format** list, select a format for the report.
You can save the report in the following formats: Portable Document Format (PDF), HTML, and Microsoft Word.
 7. To specify an alternative location to save the report, click **Browse**, and then 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).

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. You can generate legacy reports from Fortify Extension for Visual Studio or from the command line (ReportGenerator utility). For information about how to generate legacy reports from the command line, see the *OpenText™ Static Application Security Testing User Guide*.

The following sections describe the default reports and report templates, instructions on how to modify existing reports, and how to create your own reports.

Generating Legacy Issue 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 and XML files.

To generate a legacy issue report:

1. From the Fortify extension menu, select **Generate Legacy Report**.
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 or XML).
7. Click **Save**.

The Fortify Extension for Visual Studio generates the report in the format you selected.

Legacy Report Templates

This section describes how to select and edit a legacy report template. You can modify legacy report templates from the Generate Legacy Report dialog box, or you can edit report templates directly in XML (see ["Legacy Report Template XML Files" on page 79](#)). If you or another user have edited or created additional legacy report templates, you might not see the default report templates described in this section.

The legacy report templates include:

- **Fortify Security Report**—A mid-level report that provides comprehensive information about the analysis performed and the high-level details of the audit that was performed. It also provides a high-level description and examples of categories that are of the highest priority.
- **Fortify Developer Workbook**—Provides 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.
- **OWASP Top Ten <year>**—Provides high-level summaries of uncovered vulnerabilities organized based on the top ten issues that the Open Web Security Project (OWASP) has identified.
- **Fortify Scan Summary**—Provides high-level information based on the category of issues that OpenText SAST found as well as a project summary and a detailed project summary

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

Opening Legacy Report Templates

To open a report template:

1. From the Fortify extension menu, select **Generate Legacy Report**.
2. Select a report template from the **Report** list.

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

Selecting Legacy Report Sections

You can choose which sections to include in the report.

To select the sections to include in a report:

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

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

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.

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 include in the report.
3. Edit the text and text variables.

As you edit text subsections, you can insert variables that are defined when you run the report. The following table describes these variables.

Variable	Description
\$AUDIT_GUIDE_SUMMARY\$	List of filters created with answers to Audit Guide Wizard questions
\$CLASSPATH_LISTING\$	JAR files used in the scan, one relative path per line
\$COMMANDLINE_ARGS\$	Complete list of command-line options (same format as project summary)
\$FILE_LISTING\$	List of files scanned, each file in the following format: <code><relative_file_path> # Lines # kb <timestamp></code>
\$FILTERSET_DETAILS\$	List of filters used by the current filter set
\$FILTERSET_NAME\$	Name of the current filter set
\$FORTIFY_SCA_VERSION\$	OpenText SAST version
\$LIBDIR_LISTING\$	Libdirs specified during scan, one relative path per line
\$TLOC\$	Total lines of code
\$NUMBER_OF_FILES\$	Total number of files scanned
\$PROJECT_BUILD_LABEL\$	Build label of project

Variable	Description
\$PROJECT_NAME\$	Build ID
\$PROPERTIES\$	Complete list of properties set during analysis phase (same format as project summary)
\$RESULTS_CERTIFICATION\$	Complete certification detail with list of validity on a per file basis (same format as project summary)
\$RESULTS_CERTIFICATION_SUMMARY\$	Short certification description (same format as project summary)
\$RULEPACKS\$	Complete list of Rulepacks used during the analysis (same format as project summary)
\$SCAN_COMPUTER_ID\$	Hostname of the machine on which the scan was performed
\$SCAN_DATE\$	Date of the analysis with the default formatting style for the locale
\$SCAN_SUMMARY\$	Summary of the codebase scanned in the format: # files, # lines of code
\$SCAN_TIME\$	Time of the analysis phase
\$SCAN_USER\$	User name of the user who performed the scan
\$SOURCE_BASE_PATH\$	Source base path of the codebase
\$TOTAL_FINDINGS\$	Number of issues, excluding suppressed or removed issues
\$VERSION_LABEL\$	Label of the scanned project (available only if the OpenText SAST - 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 the 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 with a search query.
For more details about the search syntax, see ["Searching for Issues" on page 48](#).

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 a search query.
For information about search syntax, see ["Searching for Issues" on page 48](#).
4. Select the chart format (table, pie, or bar).

Saving Legacy Report Templates

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

To save settings as a report template:

1. From the Fortify extension menu, select **Generate Legacy Report**.
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. From the Fortify extension menu, select **Generate Legacy Report**.
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**.

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 `<tools_install_dir>\Core\config\reports`.

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

Adding Legacy Report Sections

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

```
<ReportSection enabled="true" optionalSubsections="true">
  <Title>Results Outline</Title>
  <SubSection enabled="true">
    <Title>Overall number of results</Title>
    <Description>Results count</Description>
    <Text>The scan found $TOTAL_FINDINGS$ issues.</Text>
  </SubSection>
  <SubSection enabled="true">
    <Title>Vulnerability Examples by Category</Title>
    <Description>Results summary for critical and high priority issues.
      Vulnerability examples are provided by category.
    </Description>
    <IssueListing limit="1" listing="true">
      <Refinement>[fortify priority order]:critical OR
        [fortify priority order]:high</Refinement>
      <Chart chartType="list">
        <Axis>Category</Axis>
      </Chart>
    </IssueListing>
  </SubSection>
</ReportSection>
```

In 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 multiple subsections.

Adding Report Subsections

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

Adding Text Subsections

In a text subsection, you can include the Title element, the Description element, and the Text element. In the Text element, you can provide the default content although 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 76](#). 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 element, the Description element, and the IssueListing element. In the IssueListing element, you can define the default content for the limit and set listing to true. You can include the Refinement element either with or without a default statement although the user can edit the content before they generate a report. To generate a results list, the Chart element's attribute chartType is set to list. You can also include the Axis element. The following XML is the Vulnerability Examples by Category subsection in the Results Outline section:

```
<SubSection enabled="true">
  <Title>Vulnerability Examples by Category</Title>
  <Description>Results summary for critical and high priority issues.
    Vulnerability examples are provided by category.
  </Description>
  <IssueListing limit="1" listing="true">
    <Refinement>[fortify priority order]:critical OR
      [fortify priority order]:high</Refinement>
    <Chart chartType="list">
      <Axis>Category</Axis>
    </Chart>
  </IssueListing>
</SubSection>
```

In this example, the results list subsection title is Vulnerability Examples by Category. The text Results summary for critical and high priority issues. Vulnerability examples are provided by category. is used to describe the purpose of the subsection. This subsection lists (listing=true) one issue (limit="1") per category (the value of the Axis element) where there are issues matching the statement [fortify priority order]:critical OR [fortify priority order]:high (the value of the Refinement element).

Adding Chart Subsections

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

The following code shows an example of a chart subsection:

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

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

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 Fortify Software Security Center.

Opening Audit Projects

To open an audit project file:

1. Open a solution or project.
2. From the Fortify extension menu, select **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 folder, and then click **OK**.

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

Configuring the Default Filter Set for Auditing

You can specify a default filter set to use with an audit project. Fortify Extension for Visual Studio uses this filter set every time you audit the project. The filter set must exist in the project template. Otherwise, the default filter set available in the audit project's template is used.

To configure a default filter set for an audit project:

1. From the Fortify extension menu, select **Options**.
2. In the left pane, select **Project Configuration**.
3. Select the **Audit Options** tab.
The **Audit Options** tab is only visible if you have an audit project open.
4. Specify the scope of the configuration by doing one of the following:
 - To configure the settings for the projects in the open solution only, select the **Enable Project Specific Settings** check box.
 - To change the default audit configuration for all projects scanned from this Visual Studio instance, click **Configure Defaults**.
5. Make sure that **Override default filter set on start with** is selected, and then select a filter set from the list.

See Also

["Creating a Filter Set" on page 64](#)

["Managing Folders" on page 67](#)

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.

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 OpenText SAST options were the same, and the scan was performed with the same set of OpenText Secure Coding Rulepacks and custom Rulepacks.

Merging Audit Data

To merge audit projects:

1. Open an audit project in Visual Studio.
2. From the Fortify extension menu, select **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 in 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. From the Fortify extension menu, select **Options**.
 - b. In the left pane, select **Server Configuration**.
 - c. Under **Software Security Center**, specify the **Server URL** for Fortify Software Security Center.

Tip: Click **Test Connection** to confirm that the URL is valid, and you can successfully connect to the Fortify Software Security Center server.

- d. Click **OK**.
2. If you already have an audit project open, close it.
 3. From the Fortify extension menu, select **Open Collaborative Audit**.
 4. If prompted, type your Fortify Software Security Center login credentials.
For information about logging into Fortify Software Security Center, see ["Logging in to Fortify Software Security Center" on page 18](#).
 5. 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.
 6. Audit the project as described in ["Auditing Issues" on page 58](#).
 7. When you complete the audit, select **Upload Audit Project** from the Fortify extension menu.

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

Uploading Results to Fortify Software Security Center

You can manually upload analysis results to Fortify Software Security Center any time after a scan is completed. However, before you do, a corresponding application version must already exist in Fortify Software Security Center.

Important! If Fortify Software Security Center uses an SSL connection from an internal certificate authority or a self-signed certificate, you must import the Fortify Software Security Center certificate into the local Windows certificate store.

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

To upload results to Fortify Software Security Center:

1. If necessary, configure a connection to Fortify Software Security Center:
 - a. From the Fortify extension menu, select **Options**.
 - b. In the left pane, select **Server Configuration**.
 - c. Under **Software Security Center**, specify the **Server URL** for Fortify Software Security Center.

Tip: Click **Test Connection** to confirm that the URL is valid, and you can successfully connect to the Fortify Software Security Center server.

- d. Click **OK**.
2. From the Fortify extension menu, select **Upload Audit Project**.
 3. If prompted, type your Fortify Software Security Center credentials.

For information about logging into Fortify Software Security Center, see ["Logging in to Fortify Software Security Center" on page 18](#).

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.

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. For a list of supported bug tracker applications, see the *OpenText™ Application Security Software System Requirements* document.

Filing Bugs to Azure DevOps Server

The Fortify Extension for Visual Studio supports integration with bug tracker applications so that you can file bugs directly to Azure DevOps Server. For a list of supported versions, see the *OpenText™ Application Security Software System Requirements* document.

To file a bug to Azure DevOps Server:

1. Open an audit project in Visual Studio.
2. In the Analysis Results window, select an issue.
3. In the Issue Auditing window, select the **Audit** tab, and then click **File Bug**.
4. If this is the first time you have filed a bug, the Select Bug Tracker Integration dialog box opens. Do the following:
 - a. Select **Azure DevOps Server**, and then click **Select**.
 - b. Click **Servers**, and then click **Add**.
 - c. In the Add Azure DevOps Server dialog box, provide the necessary information, and then click **OK**.
 - d. Click **Close** to close the Add/Remove DevOps Server dialog box.
 - e. In the Connect to Azure DevOps Server dialog box, select a server, a Team Project Collection, and a Team Project, and then click **Connect**.
5. Specify the following information for your installation:
Project: <team_project_name>
WorkItem Type: **Bug**
6. Click **OK**.
7. (Optional) In the Azure DevOps Server dialog box, provide the information to file the bug report.
8. Click **File Bug**.

Troubleshooting

The following topics provide information about how to troubleshoot problems you might encounter working with the Fortify Extension for Visual Studio.

Enabling Debug Mode

If you encounter any errors, you can enable debug mode to help troubleshoot. When you enable debug mode, Fortify Extension for Visual Studio writes additional information to the log files.

To enable debug mode:

1. Navigate to the `<tools_install_dir>\Core\config` folder and open the `fortify.properties` file in a text editor.
2. You can either enable debug mode for all OpenText Application Security 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 <code>true</code> , all the OpenText Application Security Software components run in debug mode.
<code>#com.fortify.VS.Debug=false</code>	If set to <code>true</code> , the Fortify Extension for Visual Studio runs in debug mode.

Locating the Log Files

To get help with diagnosing an issue, send the log files to Customer Support. On Windows systems, the log files are in the following folders:

- `C:\Users\<username>\AppData\Local\Fortify\VS<VSversion>-<version>\log`
- `C:\Users\<username>\AppData\Local\Fortify\sca<version>\log`
The log files in this folder are only available if you analyze the code locally with OpenText SAST.
- `C:\Users\<username>\AppData\Local\Fortify\scancentral-<version>\log`
The log files in this folder are only available if you analyze the code with Fortify ScanCentral SAST.

Chapter 3: Remediating Results from Fortify Software Security Center

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

This section contains the following topics:

Requirements for Remediating Results	87
Opening a Fortify Software Security Center Application	88
Viewing Analysis Results from Fortify Software Security Center	88
Viewing Issue Information	99
Locating Issues in Source Code	102
Auditing Analysis Results	103

Requirements for Remediating Results

To remediate results from Fortify Software Security Center, you must have the following:

- A Fortify Software Security Center URL
- If your Fortify Software Security Center server uses an SSL connection from an internal certificate authority or a self-signed certificate, you must import the Fortify Software Security Center certificate into the local Windows certificate store.
- A user account on the Fortify Software Security Center server that has permission to access application versions

To log into Fortify Software Security Center, you can use a user name and password or an authentication token.

- To audit issues in the analysis results, your user account must have audit permission.

In addition to audit permissions, the following audit tasks require additional permissions:

- To add comments to issues or assign values to custom tags that require comments, your user account must have the permission to comment on issues.
- To override issue priority, your user account must have the permission to edit restricted custom tag values.

Note: You do not need to specify a Fortify license file for the Fortify Extension for Visual Studio. Only Fortify Software Security Center requires a license file.

Opening a Fortify Software Security Center Application

To open an application version in the Fortify Extension for Visual Studio:

1. If you have not already done so, configure a connection to a Fortify Software Security Center server:
 - a. From the Fortify extension menu, select **Options**.
 - b. In the left pane, select **Server Configuration**.
 - c. Under **Software Security Center**, specify the **Server URL** for Fortify Software Security Center.

Tip: Click **Test Connection** to confirm that the URL is valid, and you can successfully connect to the Fortify Software Security Center server.

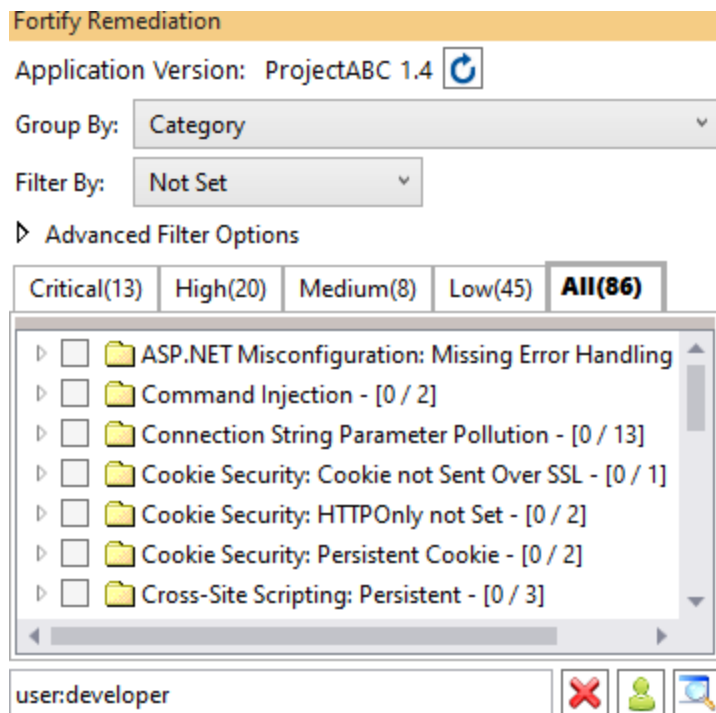
- d. Click **OK**.
2. From the Fortify extension menu, select **Connect to SSC**.
 3. If prompted, type your Fortify Software Security Center login credentials.
For information about logging into Fortify Software Security Center, see "[Logging in to Fortify Software Security Center](#)" on page 18.
 4. In the Select Application Version dialog box, select an application version to open, and then click **OK**.

The Fortify Extension for Visual Studio downloads the analysis results for the application version from Fortify Software Security Center.

Note: To open a different application version in Fortify Software Security Center, reselect **Fortify > Connect to SSC** from the Fortify extension menu.

Viewing Analysis Results from Fortify Software Security Center

After you open an application version, you can see the analysis results in the Fortify Remediation window. This window displays all security issues, organized in folders (color-coded tabs) in an issue list.



Folders contain logically defined sets of issues. For example, the **Critical** folder contains all critical issues for an application. Similarly, the **Low** folder contains all low-priority issues.

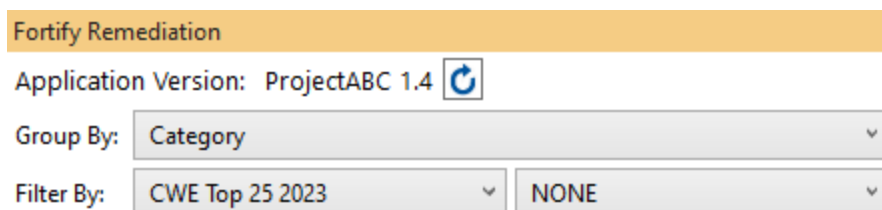
Filters determine which issues are visible. The filters are organized into distinct groups called filter sets. An issue template can contain definitions for multiple filter sets. You can use multiple filter sets to change the sorting and visibility of issues.

To remediate issues, the project you have open in Visual Studio must correspond to the application version you opened in Fortify Software Security Center (see ["Opening a Fortify Software Security Center Application" on the previous page](#)).

Viewing and Selecting Issues


To view and select issues in an opened application version:

1. From the **Group By** list, select an attribute for sorting issues in all visible folders into groups. The default grouping is **Category**. For a description of the available **Group By** attributes, see ["Grouping Issues" on page 91](#).
2. To filter the issues within the selected grouping:
 - a. From the **Filter By** list, select a filter category.




- b. To refine the issues further, select a filter option from the list to the right of the selected filter category.

Fortify Remediation


Application Version: ProjectABC 1.4 

Group By: Category

Filter By: CWE Top 25 2023 [1] CWE ID 787

3. By default, issues assigned to your Fortify Software Security Center user name are visible. To see issues assigned to all users, click the **Clear** button .

To see issues assigned to a specific user, do the following:

- a. Click the **Select User** button .
- b. In the Select User dialog, select a user name, and then click **OK**.

Only issues assigned to the selected user are shown in the Fortify Remediation window.

Tip: To see only issues assigned to you, from the **Filter By** list, select **Assignments** and **My Assignments**.

4. Click a folder (tab) to view the associated issues.

Note: The folders shown depends on your **Group By**, **Filter By**, **Assigned User**, and **Filter Set** selections. It is possible that not all folders are shown. The folders shown also depends on the issue template associated with the application version.

The following table describes the folders that are visible when the **Security Auditor View** filter set is selected.

Folder	Description
Critical	This folder contains issues that have a high impact and a high likelihood of occurring. Issues at this risk level are easy to discover and to exploit and represent the highest security risk to a program. Remediate critical issues immediately.
High	This folder contains issues that have a high impact and a low likelihood of occurring. High-priority issues are often difficult to discover and exploit but can result in much asset damage. They represent a significant security risk to a program. Remediate these issues with the next patch release.
Medium	This folder contains issues that have a low impact and a high likelihood of exploitation. Medium-priority issues are easy to discover and exploit but often result in little asset damage. These issues represent a moderate security risk to a program. Remediate these issues as time permits.

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

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

- Expand the **Advanced Filter Options** section to access the filter set and issue visibility settings.
- From the **Filter Set** list, 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 you opened.

- Click to expand a folder and view the associated issues.

The Fortify Extension for Visual Studio retrieves the corresponding issues from Fortify Software Security Center.
- Click an issue name to view the issue information.

Note: Selecting the check box for an issue opens the **Bulk Audit** tab where you can add audit information for multiple issues.

See Also

["Grouping Issues" below](#)

["Searching for Issues" on page 94](#)

Grouping Issues

The items visible in the Fortify Remediation window issues list vary depending on the selected grouping attribute. The attribute you select from the **Group By** list sorts issues in all visible folders into subfolders. Use the **Group By** attributes to group and view the issues in different ways. The following table describes the available **Group By** attributes.

Attribute	Description
Analysis	Groups issues by the audit analysis value assigned, 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 Application Defender can protect the vulnerability category.
Category	Groups issues by vulnerability category. This is the default setting.
<custom_tagname>	Groups issues by the selected custom tag.
Engine Priority	Groups issues based on the original priority value determined by the engine that identified the issue.
File Name	Groups issues by file name.
Folder	Groups issues by folders defined in the issue template.
Fortify Priority Order	Groups issues as Critical, High, Medium, and Low based on issue priority.
Introduced date	Groups issues by the date the issue was first detected.
Issue State	Groups audited issues by whether the issue is an open issue or not an issue based on the level of analysis set for the primary tag. Values equivalent to suspicious and exploitable are considered open issue states.
Kingdom	Groups issues by the Seven Pernicious Kingdoms classification.
Manual	Groups issues by whether they were manually created by penetration test tools, and not automatically produced by a web crawler such as OpenText™ Dynamic Application Security Testing.
<metadata_listname>	Groups issues using the alternative metadata external list names (for example, OWASP Top 10 <year>, CWE, PCI SSF <version>, STIG <version>, and others).

Attribute	Description
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 group and the others are displayed in the UPDATED group. If removed issues are visible, issues not found in the latest scan are displayed in the REMOVED list.
Package	Groups issues by package or namespace. Does not appear for projects for which this option is not applicable, such as C projects.
Primary Context	Groups issues where the primary location or sink node function call occurs in the same code context.
Priority Override	Groups issues by the Priority Override tag value assigned.
Sink	Groups issues that share the same dataflow sink functions.
Source	Groups issues that share the same dataflow source functions.
Source Context	Groups dataflow issues that have the source function call contained in the same code context.
Source File	Groups dataflow issues by the source code file where the taint originated.
Status	Groups issues by the audit status (Reviewed , Unreviewed , or Under Review).
Taint Flag	Groups issues by the taint flags that they contain.
URL	Groups dynamic issues by the request URL.

Customizing Issue Visibility

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

To customize the display of hidden, removed, and suppressed issues:

1. In the Fortify Remediation window, expand the **Advanced Filter Options** section.
2. Select or clear the following options:
 - To display all hidden issues, select **Show Hidden**.

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

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.

The Fortify Remediation window displays issues based on your selection.

Note: You can also specify the issue visibility settings from the Options dialog box (from the Fortify extension menu, select **Options**, and then select **Remediation Configuration** in the left pane).

Searching for Issues

In the Fortify Remediation window, you can use the search box located below the issues list to search for issues.

To perform a search, type a search query in the search box, and then press **Enter**.



The Fortify Remediation window displays the search results.

See Also

["Search Syntax" below](#)

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

Search Syntax

To indicate the type of comparison to perform for a search in the Fortify Remediation window, 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 (" ")
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

Comparison	Description
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" below](#).

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. 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.

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

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

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

Search Modifier (Issue Attribute)	Description
accuracy	Searches for issues based on the accuracy value specified (0.1 through 5.0).

Search Modifier (Issue Attribute)	Description
analysis	Searches for issues that have the specified audit analysis value such as exploitable, not an issue, and so on.
[analysis type]	Searches for issues by analyzer product such as SCA and WEBINSPECT.
analyzer	Searches the issues for the specified analyzer such as control flow, data flow, structural, and so on.
[app defender protected] (def)	Searches for issues based on whether Application Defender can protect the vulnerability category (protected or not protected).
audience	Searches for issues based on intended audience such as dev, targeted, medium, broad, and so on. Note: This metadata is legacy information that is no longer used and will be removed in a future release. OpenText recommends that you do not use this search modifier.
audited	Searches the issues to find true if the primary tag is set and false if the primary tag is not set. The default primary tag is the Analysis tag.
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. OpenText SAST calculates the confidence value based on the number of assumptions made in code analysis. The more assumptions made, the lower the confidence value.
<custom_tagname>	Searches for issues based on the value of the specified custom tag.

Search Modifier (Issue Attribute)	Description
	<p>You can search a list-type custom tag using a range of values. The values of a list-type custom tag are an enumerated list where the first value is 0, the second is 1, and so on. You can use the search syntax for a range of numbers to search for ranges of list-type custom tag values. For example, <code>analysis:[0,2]</code> returns the issues that have the values of the first three Analysis values, 0, 1, and 2 (Not an Issue, Reliability Issue, and Bad Practice).</p> <p>To search for a specific date in a date-type custom tag, specify the date in the format: <code>yyyy-mm-dd</code>.</p> <p>To search for issues that have no value set for a custom tag, use <code><none></code> as the search term. For example, to search for all issues that have no value set in the custom tag labeled Target Date, type: <code>[Target Date]:<none></code>.</p>
<code>dynamic</code>	Searches for issues that have the specified dynamic hot spot ranking value.
<code>[engine priority]</code>	Searches for issues based on the original priority value determined by the engine that identified the issue.
<code>file</code>	Searches for issues where the primary location or sink node function call occurs in the specified file path.
<code>[fortify priority order]</code>	Searches for issues that have a priority level that matches the specified issue priority. Valid values are <code>critical</code> , <code>high</code> , <code>medium</code> , and <code>low</code> .
<code>historyuser</code>	Searches for issues that have audit data modified by the specified user.
<code>impact</code>	Searches for issues based on the impact value specified (0.1 through 5.0).
<code>[instance id]</code>	Searches for an issue based on the specified instance ID.
<code>[issue age]</code>	Searches for the issue age, which is <code>new</code> , <code>updated</code> , <code>reintroduced</code> , or <code>removed</code> .

Search Modifier (Issue Attribute)	Description
[issue state]	Searches for audited issues based on whether the issue is an open issue or not an issue (determined by the level of analysis set for the primary tag).
kingdom	Searches for all issues in the specified kingdom.
likelihood	Searches for issues based on the specified likelihood value (0.1 through 5.0).
line	Searches for issues on the primary location line number. For dataflow issues, the value is the sink line number. Also see "sourceline" on 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.
<metadata_listname>	Searches for issues based on the value of the specified metadata external list. Metadata external lists include [owasp top ten <year>], [cwe top 25 <version>], [pci ssf <version>], [stig <version>], and others.
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.
[priority override]	Searches for all issues that have the specified Priority Override tag value. Valid values are critical, high, medium, and low.

Search Modifier (Issue Attribute)	Description
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.
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 dataflow issues with the source function call that the specified file contains. Also see " file " on page 97.
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.
url	Searches for issues based on the specified URL.
user	Searches for issues assigned to the specified user.

Viewing Issue Information

After you select an issue, the Fortify Extension for Visual Studio displays the issue-specific content on the **Audit**, **Recommendations**, **Details**, and **History** tabs. If you select multiple issues, Fortify Extension for Visual Studio displays the **Bulk Audit** tab (see "[Auditing Multiple Issues](#)" on page 104).


Audit Tab

The **Audit** tab provides a dashboard of analysis information for the selected issue.

Note: Any changes you make on the **Audit** tab are automatically uploaded to the application version in Fortify Software Security Center.


Audit
Recommendations
Details
History

Priority: **Medium**

User: 
File Path: Content/About.aspx

Analysis: Not set

The file About.aspx on line 15 links to a third-party site over an unencrypted channel.

01101 About.aspx:15
 About.aspx:15

The following table describes the **Audit** tab features.

Element	Description
User	The user assigned to the selected issue. If the box is empty, no user is assigned to the selected issue. To assign a user to the issue, see "Auditing Analysis Results" on page 103 .
Analysis	Your assessment for the selected issue. To change the assessment, select an item from the list. This is the primary tag as defined in Fortify Software Security Center. The default name of this tag is Analysis , but it might be different for your organization.
<custom_tagname>	<p>Any custom tags your organization has defined in Fortify Software Security Center. If available, these are displayed below the Analysis (primary) tag.</p> <p>If the audit results have been submitted to Fortify Audit Assistant in Fortify Software Security Center, then in addition to any other custom tags, the tab displays the following tags:</p> <ul style="list-style-type: none"> AA_Prediction—Exploitability level that Fortify Audit Assistant assigned to the issue. You cannot modify this tag value.

Element	Description
	<ul style="list-style-type: none">• AA_Confidence—Confidence level from Fortify Audit Assistant for the accuracy of its AA_Prediction value. You cannot modify this tag value.• AA_Training—Whether to include or exclude the issue from Fortify Audit Assistant training. You can modify this value. <p>For more information about Fortify Audit Assistant, see the <i>OpenText™ Application Security User Guide</i>.</p>
Comments (bottom left)	Any additional information added to the issue. For instructions on how to add comments, see "Auditing Analysis Results" on page 103 .
File Path (top right)	The path to the location of the source file for the selected issue.
Issue Abstract (below File Path)	A summary of the selected issue.
Analysis Trace (bottom right)	The items of evidence that the analyzer uncovered. The analysis trace is presented in the order it was discovered. For information about the Analysis Trace icons, see "Analysis Trace Window" on page 38 .

See Also

["Auditing Analysis Results" on page 103](#)

["Auditing Multiple Issues" on page 104](#)

Recommendations Tab

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

Details Tab

The **Details** tab provides an abstract of the selected issue description. 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 attackers can exploit it, and the potential ramifications of an attack. This section also provides custom explanations defined by your organization.
Instance ID	A unique identifier for the issue.
Primary Rule ID	The identifier for the 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 **History** tab displays a history of audit actions, including details such as the time and date, and the name of the user who modified the issue.

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. Make sure that the revision of the source code open in Visual Studio corresponds to the application version you opened on Fortify Software Security Center.

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

- From a folder in the Fortify Remediation window, select an issue.
- From the **Audit** tab, select a step from the Analysis Trace.

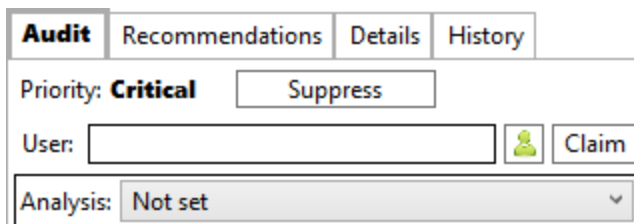
The Fortify Extension for Visual Studio jumps to the line of code that contains the security-related issue in Visual Studio.

Auditing Analysis Results


After you select and review an issue, you can assign audit information on the **Audit** tab. To audit multiple selected issues in batch, see ["Auditing Multiple Issues" on the next page](#). To see any updates to the audit information made in Fortify Software Security Center, click the **Refresh** button .

To audit an issue:

1. From a folder in the Fortify Remediation window, click an issue.
2. To assign a user to the issue, do one of the following:



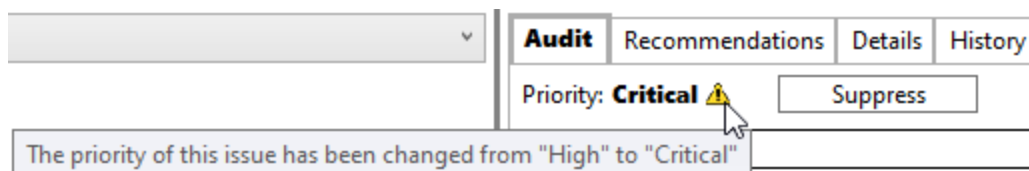
The screenshot shows the 'Audit' tab of the Fortify extension. It includes a 'Priority' dropdown set to 'Critical' with a 'Suppress' button next to it. Below that is a 'User' field with a person icon and a 'Claim' button. At the bottom is an 'Analysis' dropdown set to 'Not set'.

- Click the **Assign Issue to User** button , select a user name from the Select User dialog box, and then click **OK**.
- Click **Claim** to assign the issue to yourself.

To remove an assigned user, click the **Unassign Issue** button .

3. From the **Analysis** list, select a value that reflects your assessment of this issue.
This is the primary tag defined in Fortify Software Security Center. The default name of this tag is **Analysis**, but it might be different for your organization.
4. If the priority override capability is enabled on Fortify Software Security Center, you can override the priority value for the issue as follows:
 - a. From the **Priority Override** list, select the preferred priority value.
 - b. Explain why you changed the value in the Add Comment for Issue dialog box.
 - c. Click **OK**.

The Priority changes to the value you selected. A warning symbol indicates that the Fortify-determined priority value was changed.



This screenshot shows the 'Audit' tab with the 'Priority' dropdown set to 'Critical'. A yellow warning triangle icon is next to the 'Critical' text. Below the tab, a message box states: 'The priority of this issue has been changed from "High" to "Critical"'. The 'Suppress' button is also visible.

Note: The issue is not automatically visible in the newly assigned priority folder until the application metrics are refreshed on Fortify Software Security Center.


5. If additional custom tags are associated with the application version, specify values for those tags.

The Fortify Extension for Visual Studio displays all custom tags assigned to the application; however, you can only provide values for tags that your Fortify Software Security Center user account has permission to edit. Use the following instructions to provide values for custom tags:

- For text- and decimal-type custom tags, type the value in the box, and then click the

Save button .

Text-type custom tags accept up to 500 characters (HTML/XML tags and newlines are not allowed).

- For date-type custom tags, type a date or click the **Select Date** button  to select a date from a calendar.
- For an extensible list-type custom tag, you can add a new value to the tag by clicking **Add Value**. You can then assign this new value to the custom tag by selecting it from the list.

If any tag requires a comment, then after you provide a value for the tag, the Add Comment for Issue dialog box opens. In the **Comment** box, type a comment to describe the value you specified for the tag, and then click **OK**.

6. To add a comment for the issue audit:

- a. Click the **Add Comment** button .
- b. In the Add Comment for Issue dialog box, type a comment, and then click **OK**.


The Fortify Extension for Visual Studio makes the updates to the application version on Fortify Software Security Center.

See Also

["Suppressing Issues" on page 106](#)

["Auditing Multiple Issues" below](#)

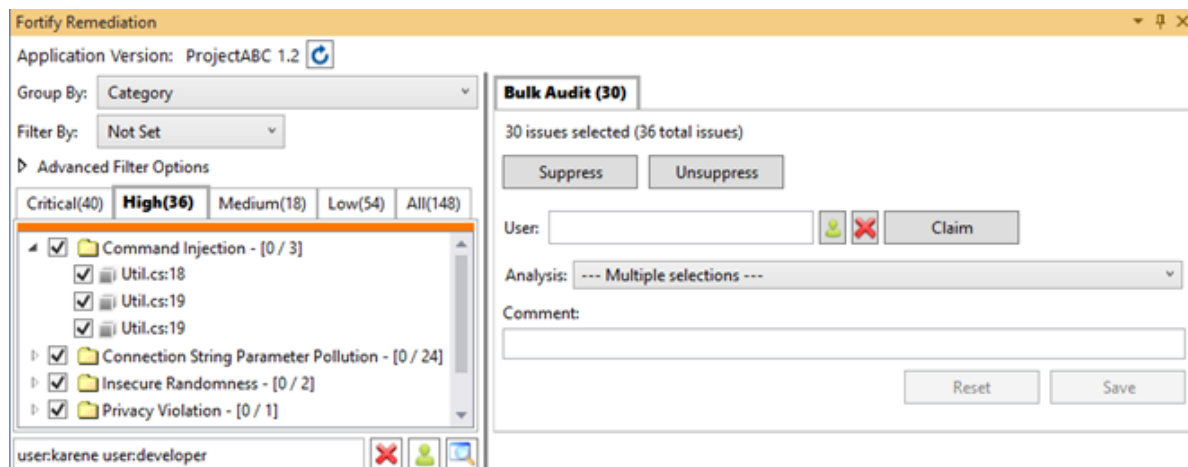
Auditing Multiple Issues

You can evaluate and assign audit information to a group of issues. To audit a single issue on the Audit tab, see ["Auditing Analysis Results" on the previous page](#). To see any updates to the audit information made in Fortify Software Security Center, click the **Refresh** button .

To audit multiple issues:


1. In the Fortify Remediation window, select multiple issues (by selecting the check box for each issue) to which you want to add the same audit information.

You can select one or more issues in the selected folder (tab). Switching to a different folder (tab) clears any previous selected issues. When you select multiple issues, Fortify Extension for Visual Studio displays the **Bulk Audit** tab.



Tip: Right-click an issue to clear all the selected issues or to select all issues in the current folder (tab).

2. To assign a user to the selected issues, do one of the following:

- Click the **Assign Issue to User** button , select a user name from the Select User dialog box, and then click **OK**.
- Click **Claim** to assign the issues to yourself.

To remove an assigned user, click the **Unassign Issue** button .

3. From the **Analysis** list, select a value that reflects your assessment of this issue.

This is the primary tag defined in Fortify Software Security Center. The default name of this tag is **Analysis**, but it might be different for your organization.


4. If the priority override capability is enabled on Fortify Software Security Center, you can override the issue priority value by doing the following:
- a. From the **Priority Override** list, select the preferred priority value.
 - b. In the box that appears below the list, type a comment to explain why you changed the value.

Note: The issues are only visible in the newly assigned priority folder after the application metrics are refreshed on Fortify Software Security Center.

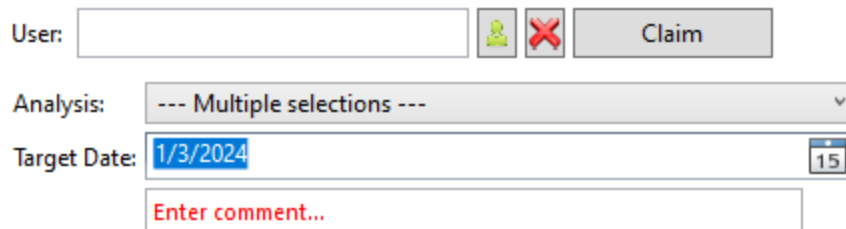
5. If additional custom tags are associated with the application version, specify values for those tags.



The Fortify Extension for Visual Studio displays all custom tags assigned to the application; however, you can only provide values for tags that your Fortify Software Security Center user account has permission to edit.

Use the following instructions to provide values for custom tags:


- For text- and decimal-type custom tags, type the value in the box.
Text-type custom tags accept up to 500 characters (HTML/XML tags and newlines are not allowed).
- For date-type custom tags, type a date or click the **Select Date** button  to select a date from a calendar.

If any tag requires a comment, then after you provide a value for the tag, you must type a comment in the comment box that appears below the tag box.



User:  

Analysis:

Target Date: 

6. To add a comment for the audit of these issues, type the content in the **Comment** box.
7. Click **Save**.

The Fortify Extension for Visual Studio makes the updates to the application version in Fortify Software Security Center.

See Also

["Suppressing Issues" below](#)

["Auditing Analysis Results" on page 103](#)

Suppressing Issues

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

To suppress an issue:

1. From a folder in the Fortify Remediation window, select one or more issues.
2. On the **Audit** or **Bulk Audit** tab, click **Suppress**.
3. (Optional) In the Suppress Issues dialog box, describe the reason for suppressing the issue.
4. Click **OK** to confirm the issue suppression.

To unsuppress an issue:

1. Make sure that suppressed issues are visible.
To display issues that have been suppressed, see ["Customizing Issue Visibility" on page 93](#).
2. From a folder in the Fortify Remediation window, select one or more suppressed issues.
3. On the **Audit** or **Bulk Audit** tab, click **Unsuppress**.
4. (Optional) In the Suppress Issues dialog box, describe the reason for unsuppressing the issue.
5. Click **OK** to confirm the issue unsuppression.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email.

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

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

Feedback on User Guide (Fortify Extension for Visual Studio 25.2.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!