Micro Focus
Fortify Extension for Visual Studio

Software Version: 21.1.0

User Guide

Document Release Date: July 2021
Software Release Date: July 2021

Legal Notices

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

https://www.microfocus.com

Warranty

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

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Documentation Updates

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

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

This document was produced on May 19, 2021. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

Contents

Preface

Contacting Micro Focus Fortify 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/solutions/application-security

About the Documentation Set

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

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

Change Log

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

Software Release / Document Version	Changes
21.1.0	Updated: • "About Analyzing the Source Code" on page 11 - Changes made to describe the new capabilities in scanning source code with Micro Focus Fortify ScanCentral SAST • "Configuring Advanced Local Scan Options" on page 24 - New option to disable merging of analysis results when you rescan a project or solution • "About Scanning with Fortify ScanCentral SAST" on page 26 - New ability to perform remote translation and scan with Fortify ScanCentral SAST • "BIRT Reports" on page 66 - Report template renamed CWE Top 25 to accommodate multiple versions now supported
20.2.0	Updated: • "Logging in to Fortify Software Security Center" on page 17 - New ability to connect to Fortify Software Security Center with an authentication token • "Updating Security Content" on page 20 - New option to update Fortify Security Content in different languages • "Configuring Advanced Local Scan Options" on page 24 - New option to specify a custom build ID for the scan • "Adding a Custom Tag" on page 59 - New ability to make a custom tag the primary tag • "BIRT Reports" on page 66 - Added a description of a new report: OWASP ASVS 4.0 • "Remediating Results from Fortify Software Security Center" on page 82 - Edited to reflect minor user interface changes • Replaced all references to Micro Focus Fortify ScanCentral with the

Software Release / Document Version	Changes
	new product name: Micro Focus Fortify ScanCentral SAST
20.1.0	Updated: - Replaced all references to Micro Focus Fortify CloudScan with the new product name: Micro Focus Fortify ScanCentral SAST - "BIRT Reports" on page 66 - Added a description of a new report: CWE Top 25 2019
19.2.0	Added: - "About Scanning with Fortify ScanCentral SAST" on page 26, "Configuring Fortify ScanCentral SAST Options" on page 27, and "Scanning Projects or Solutions with Fortify ScanCentral SAST" on page 29 - You can now offload scanning to Fortify ScanCentral SAST Updated: - "Issue Auditing Window" on page 38 - Tab names changed for consistency with Fortify Software Security Center - "BIRT Reports" on page 66 - Support added for GDPR, MISRA, and PCI SSF Compliance: Secure Software Requirements reports - "Filing Bugs to Azure DevOps Server" on page 80 - Updated for support with Azure DevOps Server - "Configuring a Connection to Fortify Software Security Center" on page 17 and "Customizing Issue Visibility" on page 88 - Options for remediation were moved to the Fortify extension **Options** menu

Chapter 1: Introduction

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

This section contains the following topics:

Fortify Extension for Visual Studio

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

Software security analysis typically consists of the following phases:

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

The Fortify Extension for Visual Studio uses Micro Focus Fortify Static Code Analyzer and Fortify Secure Coding Rulepacks to locate security vulnerabilities in your solutions and projects (includes support for the following languages: C/C++, C#, 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 Micro Focus Fortify Software Security Center to manage applications and assign specific issues to developers. You can connect with Fortify Software Security Center to review the reported vulnerabilities and implement appropriate solutions from Visual Studio.

Fortify Security Content

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

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

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

If you are using collaborative auditing with Micro Focus 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 Fortify Extension for Visual Studio. For information about updating Fortify Security Content or installing it manually, see "About Updating Security Content" on page 19.

About Analyzing the Source Code

You analyze the source code from Visual Studio at the solution or project level. A security analysis with Micro Focus Fortify Static Code Analyzer 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 the locally installed Fortify Static Code Analyzer to perform the entire analysis (translation and scan phases). For information about how to configure and run the analysis locally, see "About Scanning Locally" on page 22.

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

- Use Micro Focus 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 26.

  > **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 the locally installed Fortify Static Code Analyzer.

  To view the analysis results, configure the Fortify Extension for Visual Studio to upload the analysis results to a Micro Focus Fortify Software Security Center server (see "Remediating Results from Fortify Software Security Center" on page 82).

  Alternatively, you can use the provided job token in the Fortify ScanCentral SAST command-line interface to retrieve the analysis results (FPR) file, and then open them in Visual Studio (see "Opening Audit Projects" on page 77).

Installation

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

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

If you plan to scan your code from Visual Studio, make sure that you select the **Update security content after installation?** check box at the end of the Micro Focus Fortify Static Code Analyzer and Applications installation unless your administrator has set up an alternative way to deliver Fortify Security Content to you (see "Manually Updating Security Content" on page 21).

Upgrades

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

Related Documents

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

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

All Products

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

Document / File Name	Description
About Micro Focus Fortify Product Software Documentation About_Fortify_Docs_<*version*>.pdf	This paper provides information about how to access Micro Focus Fortify product documentation. **Note:** This document is included only with the product download.
Micro Focus Fortify Software System Requirements Fortify_Sys_Reqs_<*version*>.pdf	This document provides the details about the environments and products supported for this version of Fortify Software.
Micro Focus Fortify Software Release Notes FortifySW_RN_<*version*>.pdf	This document provides an overview of the changes made to Fortify Software for this release and important information not included elsewhere in the product documentation.
What's New in Micro Focus Fortify Software <version> Fortify_Whats_New_<*version*>.pdf	This document describes the new features in Fortify Software products.

Micro Focus Fortify ScanCentral SAST

The following document provides information about Fortify ScanCentral SAST. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website at https://www.microfocus.com/documentation/fortify-software-security-center.

Document / File Name	Description
Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide	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

Document / File Name	Description
SC_SAST_Guide_*<version>*.pdf	intends to install, configure, or use Fortify ScanCentral SAST to offload the resource-intensive translation and scanning phases of their Fortify Static Code Analyzer process.

Micro Focus Fortify Software Security Center

The following document provides information about Fortify Software Security Center. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website at https://www.microfocus.com/documentation/fortify-software-security-center.

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

Micro Focus Fortify Static Code Analyzer

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

Document / File Name	Description
Micro Focus Fortify Static Code Analyzer User Guide SCA_Guide_*<version>*.pdf	This document describes how to install and use Fortify Static Code Analyzer to scan code on many of the major programming platforms. It is intended for people responsible for security audits and secure coding.

Document / File Name	**Description**
Micro Focus Fortify Static Code Analyzer Custom Rules Guide SCA_Cust_Rules_Guide_<*version*>.zip	This document provides the information that you need to create custom rules for Fortify Static Code Analyzer. This guide includes examples that apply rule-writing concepts to real-world security issues. **Note:** This document is included only with the product download.

Chapter 2: Using the Fortify Extension for Visual Studio

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

This section contains the following topics:

Working with Fortify Software Security Center

You need to configure a connection to Micro Focus Fortify Software Security Center to accomplish 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 ways to login to Fortify Software Security Center 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 on Micro Focus Fortify Software Security Center, you need to configure your connection to Fortify Software Security Center.

To configure a connection to Fortify Software Security Center:

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

   The Fortify Software Security Center URL includes both the port number and the context path `/ssc`. For example, `http://my.domain.com:8080/ssc`.

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

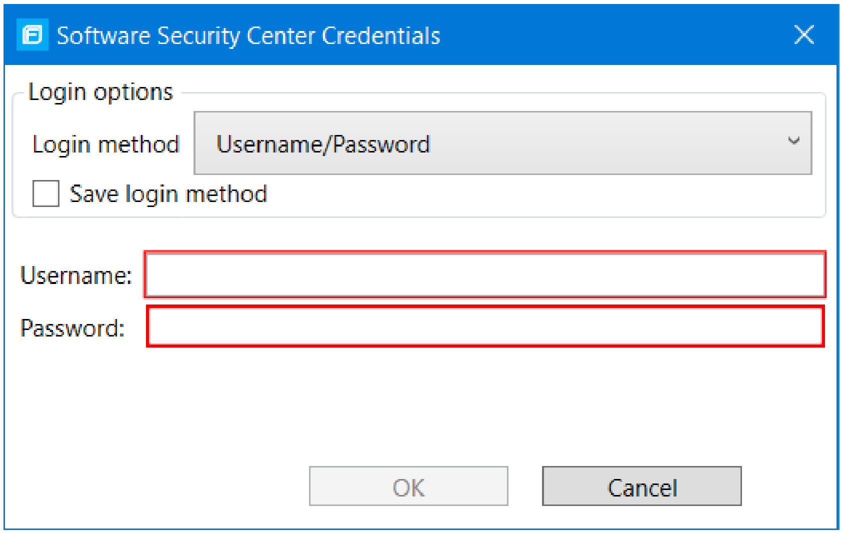
4. Click **OK**.

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.

To log in to Fortify Software Security Center:

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



Software Security Center Credentials

Login options

Login method: Username/Password

□ Save login method

Username:

Password:

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	Specify the decoded value of a Fortify Software Security Center authentication token of type ToolsConnectToken. **Note:** For instructions about how to create an authentication token from Fortify Software Security Center, see the *Micro Focus Fortify Software Security Center User Guide*
X.509 SSO	Fortify Software Security Center must be configured to use X.509 Certification-based SSO. **Note:** Your certificate must be in the current user certificate store and in the **Personal** store. a. Click **Browse for Certificate** . b. Select the certificate for the sign-on, and then click **OK**.
Kerberos SSO	Fortify Software Security Center must be configured to use SPNEGO-based Kerberos authentication. **Note:** Support for Kerberos SSO is limited to Windows systems.

4. 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 Micro Focus Fortify Software Security Center server. With synchronization to the server enabled, each time you load, merge, scan, or save your project locally on your system, the extension automatically uploads your changes to the version of your project on the server. This automatic synchronization prevents work loss during a power outage and enables you to work locally and synchronize your work when you connect later.

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:

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

3. Select the **Synchronization Options** tab.
4. Either clear the **Auto Synchronize all Projects with Server Application** check box to disable automatic synchronization or select it to enable automatic synchronization.

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

To customize the actions that trigger synchronization with the server:

1. From the Fortify extension menu, select **Options**.
2. In the left pane, select **Project Configuration**.
3. Select the **Synchronization Options** tab.
4. Select any action to exclude from automatic synchronization, and then click **OK**.

About Updating Security Content

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

- "Updating Security Content" on the next page
- "Scheduling Automatic Security Content Updates" on page 21
- "Manually Updating Security Content" on page 21

Note: Updating security content overwrites the previous security content files.

You can also import custom security content from the Fortify Extension for Visual Studio (see "Importing Custom Security Content" on page 21).

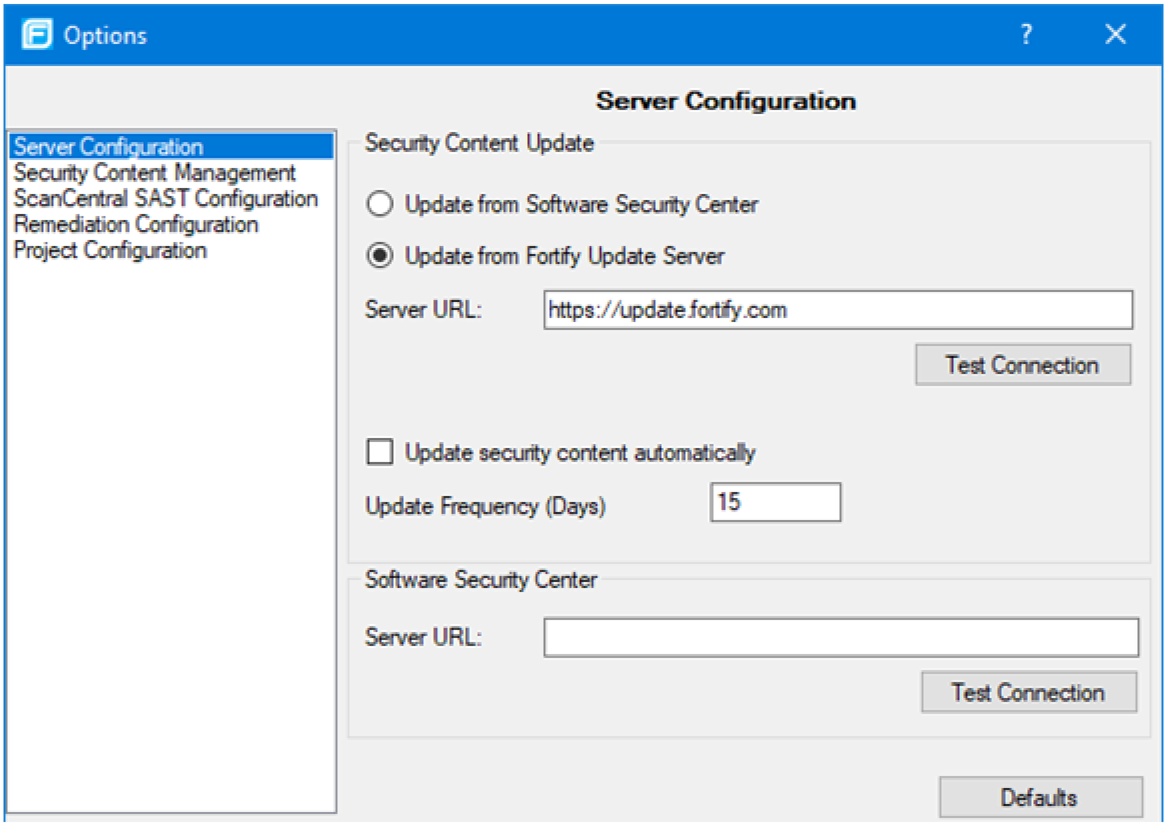
Configuring Security Content Updates

Before you update security content, configure the server information to use for security content updates. To update security content manually (without an Internet connection or Micro Focus Fortify Software Security Center), see "Manually Updating Security Content" on page 21.

To configure the security content update server:

1. From the Fortify extension menu, select **Options**.

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



Server Configuration

Security Content Update

○ Update from Software Security Center

● Update from Fortify Update Server

Server URL: https://update.fortify.com

□ Update security content automatically

Update Frequency (Days) 15

Software Security Center

Server URL:

2. Under **Security Content Update**, select one of the following:
   - To update security content from your Fortify Software Security Center instance, select **Update from Software Security Center**.
   - To specify an update server from which to update security content, select **Update from Fortify Update Server**.
3. If you selected **Update from Fortify Update Server**, do the following:
   - In the **Server URL** box, type the URL for the update server.
4. If you selected **Update from Fortify Software Security Center**, do the following:
   - Under **Software Security Center**, specify the **Server URL** for Fortify Software Security Center (for example, `http://my.domain.com:8080/ssc`).

Updating Security Content

Fortify Extension for Visual Studio updates the Fortify Security Content from the location specified in the Server Configuration options (see "Configuring Security Content Updates" on the previous page).

To update security content:

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

3. (Optional) From the **Locale** list, select the language you want for the Fortify Security Content.

   By default, English is the selected language.
4. Click **Update**.

   If new content is available, it is updated and listed under **Installed Fortify Security Content** and **Main External List Mappings**.
5. Click **OK**.

Scheduling Automatic Security Content Updates

To schedule automatic security content updates:

1. From the Fortify extension menu, select **Options**.
2. In the left pane, select **Server Configuration**.
3. Under **Security Content Update**, select the **Update security content automatically** check box.
4. In the **Update Frequency (Days)** box, specify how often to update the security content, and then click **OK**.

Manually Updating Security Content

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

To manually update the security content:

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

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

Importing Custom Security Content

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

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

To import custom rules:

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

   The Select Security Content dialog box opens.
4. Browse to and select a `*.xml` or `*.bin` file to import.

The imported file is listed under **Installed Custom Security Content**.

5. Click **OK** to close the Options dialog box.

About Scanning Locally

This section describes how to perform a scan of your source code on the local system. 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.

Fortify strongly recommends that you periodically update the security content, which contains Fortify Secure Coding Rulepacks and external metadata. For information about how to update the security content, see "About Updating Security Content" on page 19.

About Quick Scan Mode

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

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

Note: By default, Micro Focus 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 uploaded audit projects scanned in quick scan mode are processed. For more information, see analysis results processing rules in the *Micro Focus Fortify Software Security Center User Guide*.

You can use quick scan mode for scans that use a locally installed Fortify Static Code Analyzer. Audit quick analysis results just as you audit full analysis results. To perform a quick scan, see "Configuring Advanced Local Scan Options" on page 24.

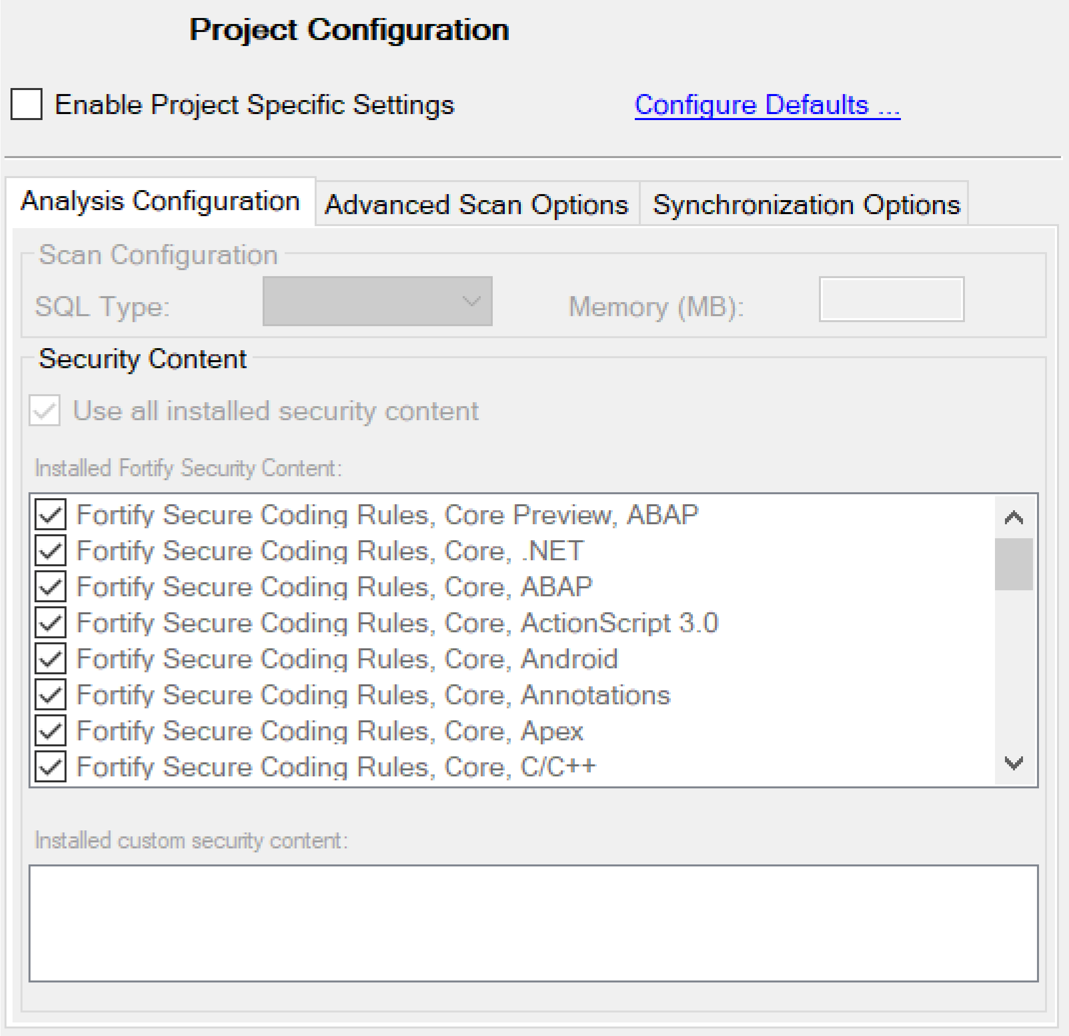
Configuring Local Scan Options

Use the analysis configuration to customize the security content, specify the SQL type, and specify the amount of memory Micro Focus Fortify Static Code Analyzer uses during a local scan.

To configure the analysis options:

1. With a solution open in Visual Studio, select **Options** from the Fortify extension menu.
2. In the left pane, select **Project Configuration**.

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



Project Configuration

☐ Enable Project Specific Settings Configure Defaults ...

Scan Configuration

SQL Type: Memory (MB):

Security Content

☑ Use all installed security content

Installed Fortify Security Content:

☑ 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
☑ Fortify Secure Coding Rules, Core, C/C++

Installed custom security content:

3. To specify the scope of the configuration, do 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, Fortify Static Code Analyzer treats SQL files as T-SQL. If your files use PL/SQL, from the **SQL Type** list, select **PL/SQL**.

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

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 Secure Coding Rulepacks and any specific custom security content that you want to use.
7. Click **OK**.

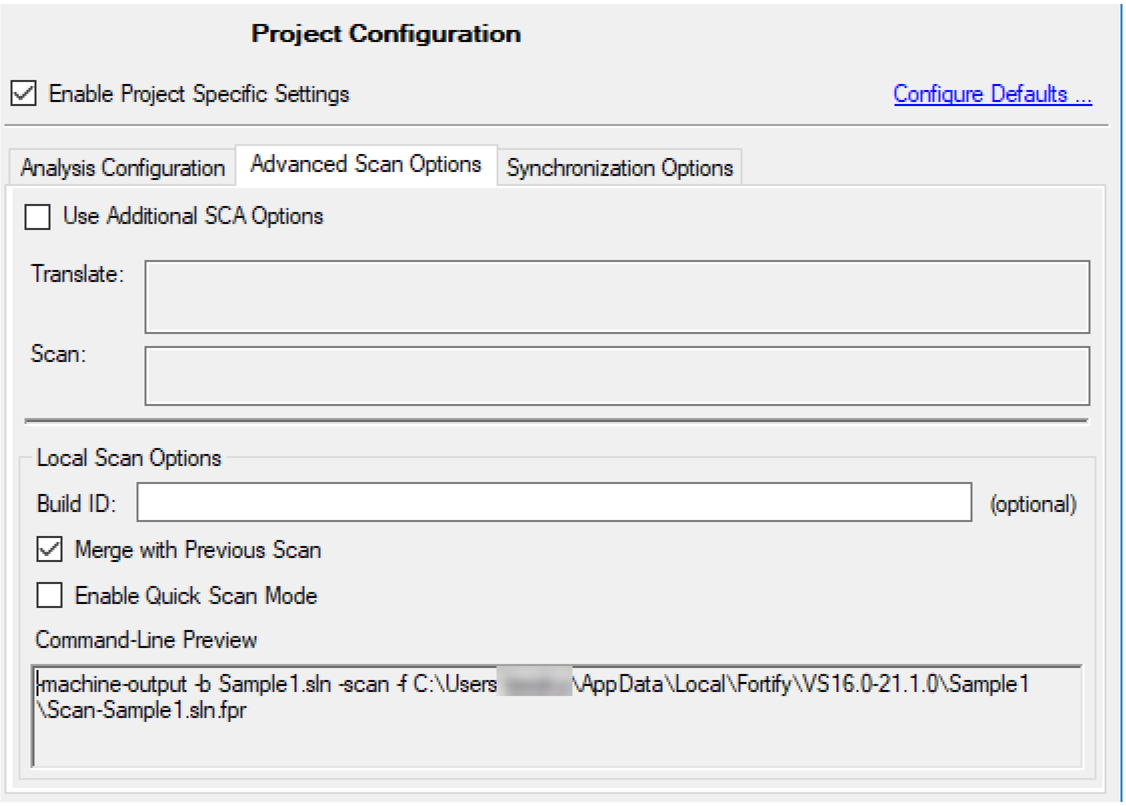
Configuring Advanced Local Scan Options

Use the advanced scan options to enable or disable quick scan mode and customize Fortify Static Code Analyzer translation and scan command-line options.

To change the advanced translation and scan options:

1. With a solution open in Visual Studio, select **Options** from the Fortify extension menu.
2. In left pane, select **Project Configuration**.
3. To specify the scope of the settings, do one of the following:
   - To customize the settings for the projects in the open solution only, select **Enable Project Specific Settings**.
   - To change the default scan settings for all projects scanned from this Visual Studio instance, click **Configure Defaults**.

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



Project Configuration

☑ Enable Project Specific Settings

☐ Use Additional SCA Options

Translate:

Scan:

Local Scan Options

Build ID: (optional)

☑ Merge with Previous Scan

☐ Enable Quick Scan Mode

Command-Line Preview

```
-machine-output -b Sample1.sln -scan -f C:\Users[redacted]\AppData\Local\Fortify\VS16.0-21.1.0\Sample1
\Scan-Sample1.sln.fpr
```

5. Select the **Use Additional SCA Options** check box and type Fortify Static Code Analyzer 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 Fortify Static Code Analyzer options and the proper syntax, see the *Micro Focus Fortify Static Code Analyzer User Guide*.

   Under **Local Scan Options**, the **Command-Line Preview** box shows the complete Fortify Static Code Analyzer 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 disable 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 22.

9. Click **OK** to save the advanced scan options.

Scanning Projects or Solutions Locally

Before you perform the scan, make sure that the active solution configuration is valid for the projects loaded in the solution. If the configuration is invalid, Fortify Static Code Analyzer cannot successfully scan the solution and a message indicating that the configuration is invalid is written to the log file.

> **Note:** Micro Focus Fortify Static Code Analyzer 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.

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

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

You can now audit the analysis results in Visual Studio. For information, see "Auditing Issues" on page 55. 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 **Fortify > Save Audit Project As**.

About Scanning with Fortify ScanCentral SAST

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

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 example, ASP.NET Web Site projects that include ASP.NET files with extensions `.aspx`, `.ascx`, `.cshtml`, `.vbhtml`, and so on and projects written in C++). For a list of languages supported with remote translation, see the *Micro Focus Fortify 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. Fortify strongly recommends that you periodically update the security content. For information about how to update the security content locally, see "About Updating Security Content" on page 19. Use the fortifyupdate utility to update security content on the ScanCentral sensor (see the *Micro Focus Fortify Static Code Analyzer User Guide*).

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

- A properly configured Fortify ScanCentral SAST installation. For more information, see the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.
- To connect to Fortify ScanCentral SAST, you need either:
  - A ScanCentral Controller URL

    Important! If the ScanCentral Controller uses an SSL connection from an internal certificate authority or a self-signed certificate, you must add the certificate to the Java Keystore for Fortify Static Code Analyzer (in `<sca_install_dir>/jre/lib/security/cacerts`). For more information, see the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

  - 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 17. For instructions on how to create an authentication token, see the *Micro Focus Fortify Software Security Center User Guide*.

    Important! If the Fortify Software Security Center or the ScanCentral Controller uses an SSL connection from an internal certificate authority or a self-signed certificate, you must add the certificate to the Java Keystore for Fortify Static Code Analyzer (in `<sca_install_dir>/jre/lib/security/cacerts`). For more information, see the *Micro Focus Fortify Software Security Center User Guide* or the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

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

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

  Note: Fortify recommends that the Fortify Software Security Center URL configured in the Server Configuration options is the same as the Fortify Software Security Center server integrated with the ScanCentral Controller.

- A Fortify Software Security Center authentication token of type ToolsConnectToken

  For instructions on how to create an authentication token, see the *Micro Focus Fortify Software Security Center User Guide*.

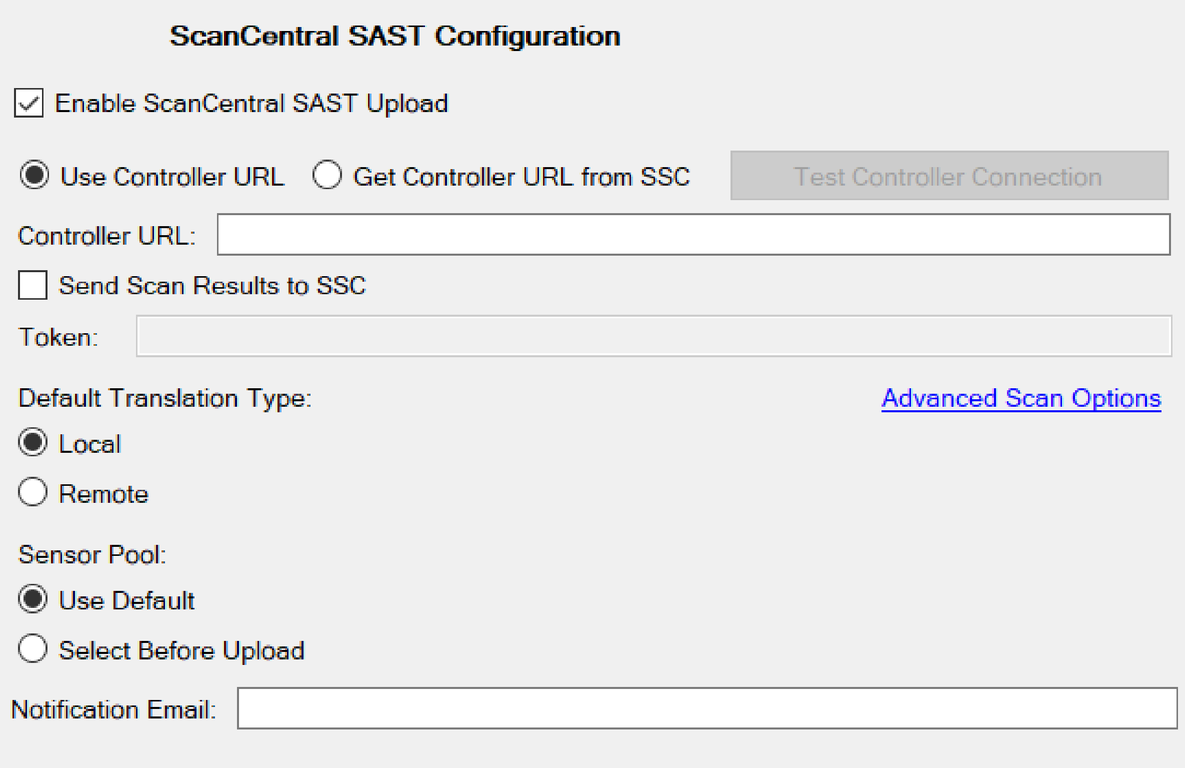
- An application and application version that exists in Fortify Software Security Center
- Permission to access the application and application version to which you want to upload

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 the translation type (local or remote), the SCA translation and scan options, 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 30.

To configure the Fortify ScanCentral SAST options:

1. From the Fortify extension menu, select **Options**.
2. In the left pane, select **ScanCentral SAST Configuration**.
3. Select **Enable ScanCentral SAST Upload**.



ScanCentral SAST Configuration

☑ Enable ScanCentral SAST Upload

● Use Controller URL ○ Get Controller URL from SSC

Controller URL:

☐ Send Scan Results to SSC

Token:

Default Translation Type:

● Local

○ Remote

Sensor Pool:

● Use Default

○ Select Before Upload

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 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 decoded token value for an authentication token of type ToolsConnectToken.

     Make sure that you have the Fortify Software Security Center URL that is associated with the ScanCentral Controller provided in the **Server Configuration** options (see "Configuring a Connection to Fortify Software Security Center" on page 17).

     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 decoded token value for an authentication token of type ToolsConnectToken.

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

6. Under **Default Translation Type**, 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.

7. (Optional) To specify Fortify Static Code Analyzer command-line options for the translation or scan phase:

   a. Click **Advanced Scan Options**.

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

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

      For detailed information about the available Fortify Static Code Analyzer options and the proper syntax, see the *Micro Focus Fortify Static Code Analyzer User Guide*.

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

8. Under **Sensor Pool**, specify whether to use the default sensor pool or be provided a list of sensor pools to choose from when you initiate a scan with Fortify ScanCentral SAST.
9. (Optional) in the **Notification Email** box, type an email address to receive job status notifications.
10. 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 27. In addition, make sure that the active solution configuration is valid for the projects loaded in the solution. If the configuration is invalid, Fortify Static Code Analyzer cannot successfully scan the solution and a message indicating that the configuration is invalid is written to the log file.

To scan a project or solution with Fortify ScanCentral SAST:

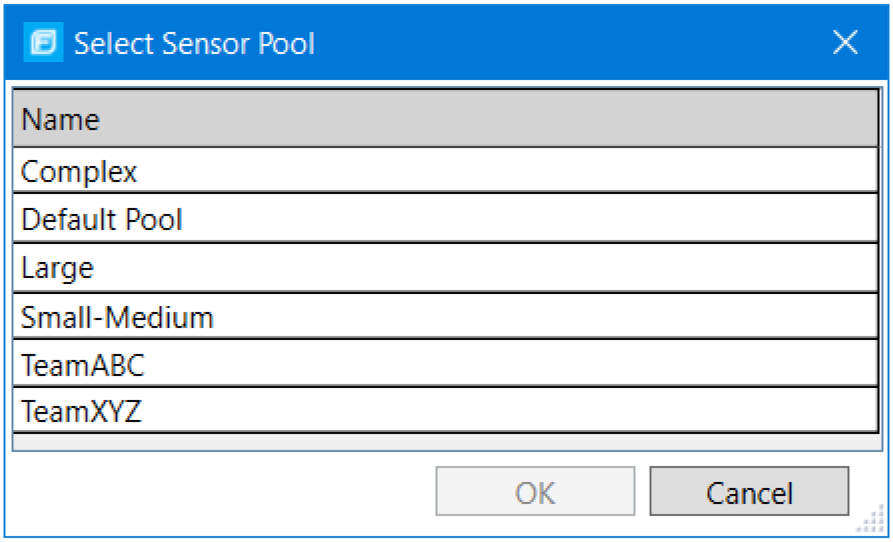
1. To start the scan with Fortify ScanCentral SAST, do one of the following:

   - To scan at the solution level, select **ScanCentral > Upload Solution** from the Fortify extension menu.

- To scan at the project level, select a project and then select **ScanCentral > Upload Project** from the Fortify extension menu.
- To scan at the solution level with custom Fortify ScanCentral SAST options for this solution, see "Advanced Scanning of Solutions with Fortify ScanCentral SAST" below.

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**.

> **Note:** The following Select Sensor Pool dialog box contains sample sensor pool names.



Name
Complex
Default Pool
Large
Small-Medium
TeamABC
TeamXYZ

To view the analysis results, you can either:

- Copy the provided job token and use it in the Fortify ScanCentral SAST command-line interface to retrieve the analysis results (see the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*). You can then open the analysis results in Fortify Extension for Visual Studio (see "Opening Audit Projects" on page 77).
- 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 78 or "Configuring a Connection to Fortify Software Security Center" on page 17).

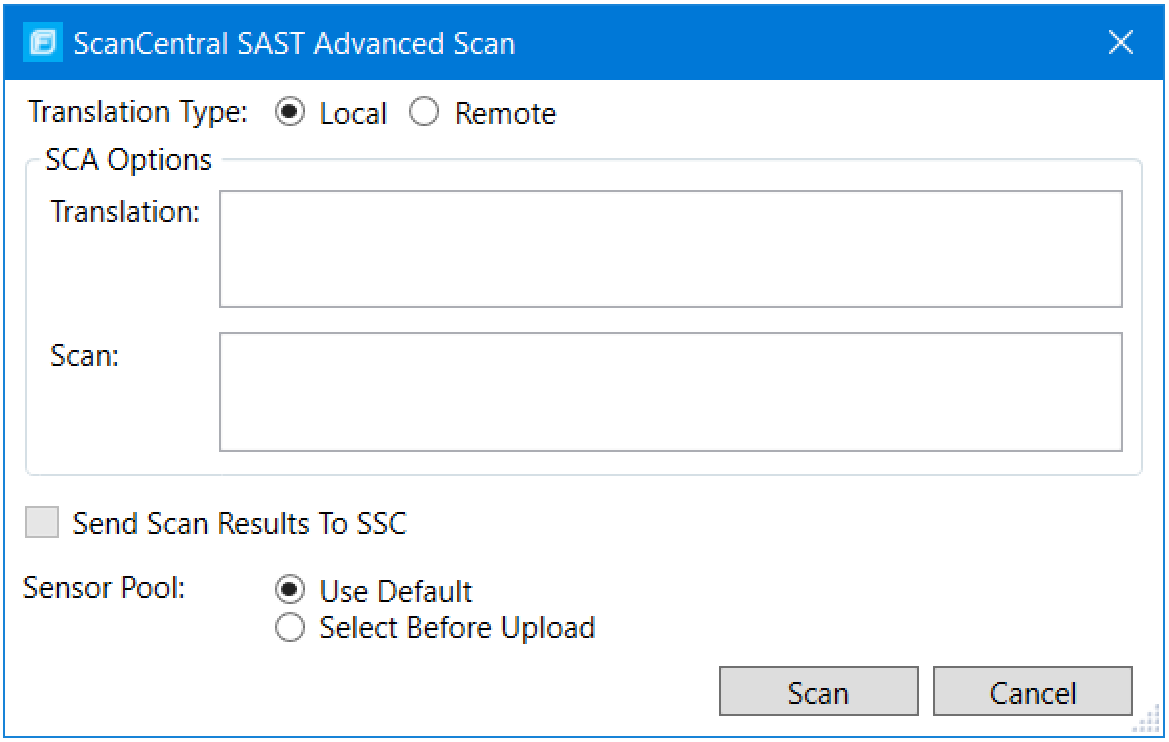
Advanced Scanning of Solutions with Fortify ScanCentral SAST

You can customize the Fortify ScanCentral SAST scan configuration for the current solution. You can adjust the translation type (local or remote), SCA 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.



ScanCentral SAST Advanced Scan

Translation Type: ● Local ○ Remote

SCA Options

Translation:

Scan:

□ Send Scan Results To SSC

Sensor Pool: ● Use Default ○ Select Before Upload

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 Fortify Static Code Analyzer command-line options for the translation or scan phase, under **SCA Options**, type command-line options for the translation and scan phase.

   For detailed information about the available Fortify Static Code Analyzer options and the proper syntax, see the *Micro Focus Fortify Static Code Analyzer User Guide*.
4. To upload the analysis results to Fortify Software Security Center, select the **Send Scan Results to SSC** check box.

   > **Important!** Make sure you have the following configured an authentication token in the **ScanCentral SAST Configuration** options (see "Configuring Fortify ScanCentral SAST Options" on page 27).
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 command-line interface to retrieve the analysis results (see the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*). You can then open the analysis results in Fortify Extension for Visual Studio (see "Opening Audit Projects" on page 77).
- 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 78 or "Configuring a Connection to Fortify Software Security Center" on page 17).

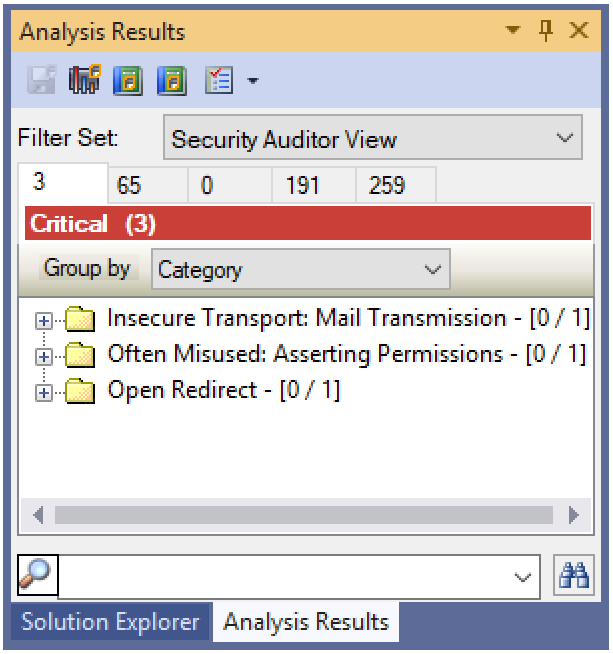
Viewing Analysis Results

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	For More Information
Analysis Results	"Analysis Results Window" on the next page
Project Summary	"Viewing Project Summary Information" on page 35
Analysis Trace	"Analysis Trace Window" on page 36
Issue Auditing	"Issue Auditing Window" on page 38

Analysis Results Window

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



Filter Set: Security Auditor View

3	65	0	191	259

Critical (3)

Group by Category

- Insecure Transport: Mail Transmission - [0 / 1]
- Often Misused: Asserting Permissions - [0 / 1]
- Open Redirect - [0 / 1]

Filter Sets

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

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

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

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

- **Quick View**—This is the default filter set for new projects. The Quick View filter set provides a view only of issues in the **Critical** folder (these have a potentially high impact and a high likelihood of occurring) and the **High** folder (these have a potentially high impact and a low likelihood of occurring). The Quick View filter set provides a useful first look at results that enables you to quickly address the most serious issues.
- **Security Auditor View**— This view 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 61.

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 63.

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, use the **Visibility** menu. For more information, see "Customizing the Issues Display" below.

Group By List

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

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

Customizing the Issues Display

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

The visibility options are as follows:

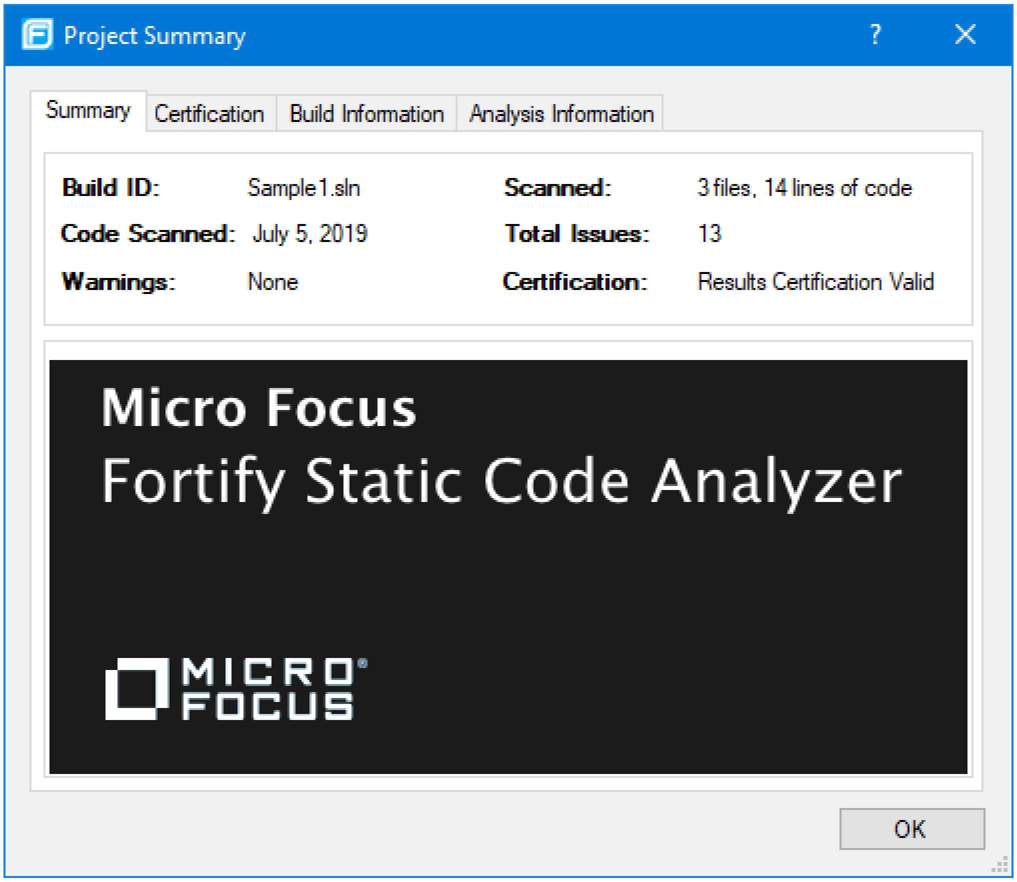
- **Show Removed Issues**—Shows all the issues you have removed or fixed. If you merged audit data into your current audit project, shows all the issues that were removed since the previous analysis.
- **Show Suppressed Issues**—Shows all the issues that you have suppressed.
- **Show Hidden Issues**—Shows 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**.



Build ID: Sample1.sln
Scanned: 3 files, 14 lines of code
Code Scanned: July 5, 2019
Total Issues: 13
Warnings: None
Certification: Results Certification Valid

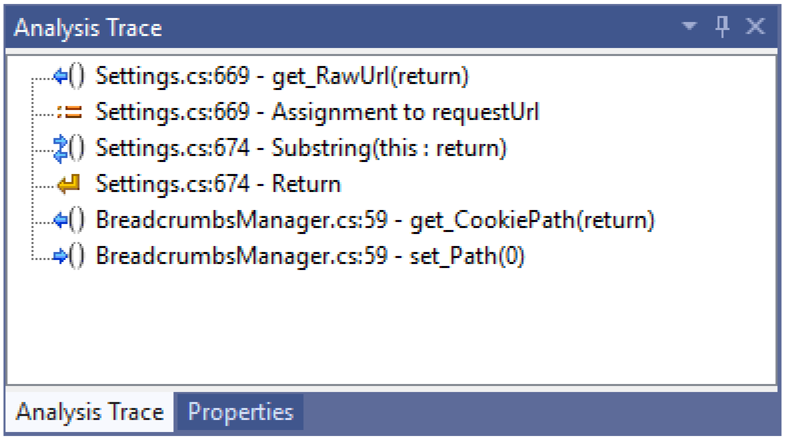
The following table describes the information provided on the Project Summary tabs.

Tab	**Description**
Summary	Displays high level audit project information.
Certification	Displays the result certification status. Results certification is a check to make sure that the analysis has not been altered since Fortify Static Code Analyzer produced it.
Build Information	Displays the following scan information: • Build details such as the build ID, number of files scanned, lines of code,

Tab	Description
	and the date of the scan, which might be different than the date the files were translated • List of files scanned with file sizes and timestamps • Libraries referenced for the scan
Analysis Information	Displays the Fortify Static Code Analyzer version, computer details, and the name of the user who performed the scan. The Analysis Information subtabs contain the following information: • Security Content—Lists information about the Rulepacks (including the Rulepack name, version, ID, and SKU) and the external metadata used in the scan • Properties—Displays the Micro Focus Fortify Static Code Analyzer properties files settings • Commandline Arguments—Displays the command-line options used to scan the project • Warnings—Lists all errors and warnings that occurred during the analysis. To view more information about an item, click it.

Analysis Trace Window

When you select an issue, the Analysis Trace window displays the trace that the analyzer used to detect the issue.



```
Settings.cs:669 - get_RawUrl(return)
Settings.cs:669 - Assignment to requestUrl
Settings.cs:674 - Substring(this : return)
Settings.cs:674 - Return
BreadcrumbsManager.cs:59 - get_CookiePath(return)
BreadcrumbsManager.cs:59 - set_Path(0)
```

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 in a function call
⇐⇒	An alias is created for a memory location
⇐▯	Data is read from a variable
⇐▯	Data is read from a global variable
↵	Tainted data is returned from a function
&	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

Icon	Description
●	Generic
01101	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:

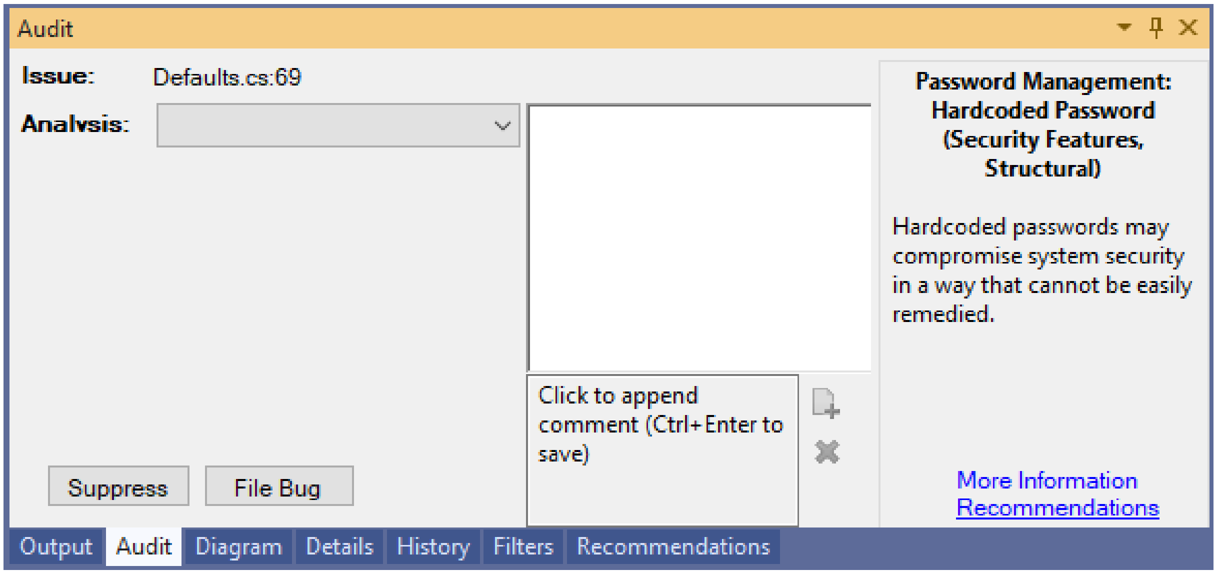
- A text node displayed in italics as a child of the trace node. This text node is expanded by default.
- An induction trace, displayed as a child of the text node.

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.



Audit

Issue: Defaults.cs:69

Analysis:

Password Management: Hardcoded Password (Security Features, Structural)

Hardcoded passwords may compromise system security in a way that cannot be easily remedied.

Click to append comment (Ctrl+Enter to save)

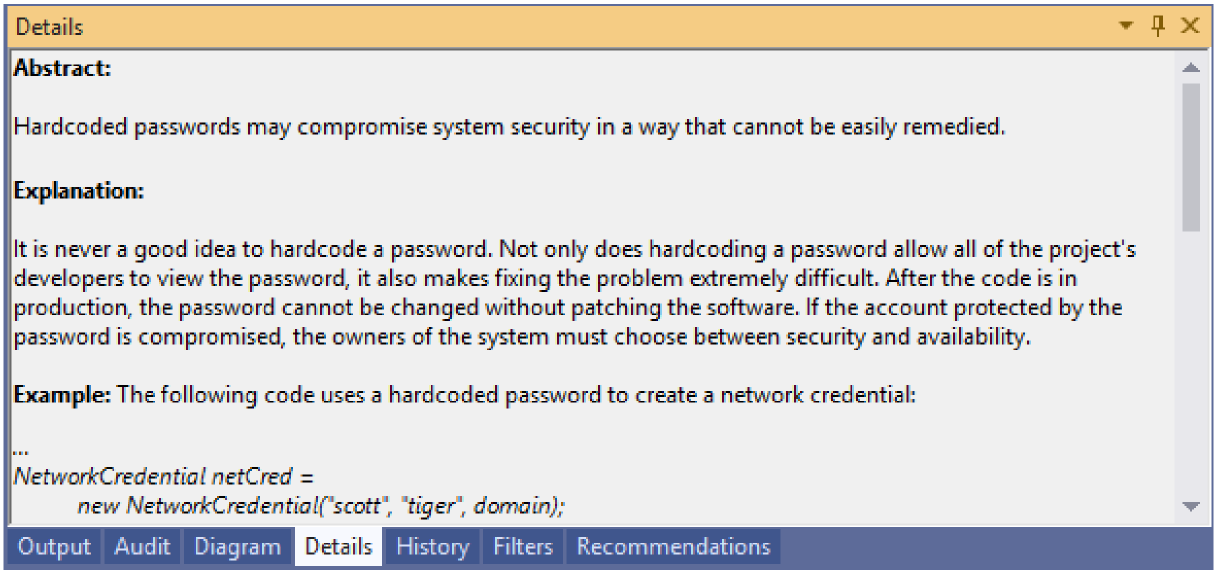
The following table describes the elements of the **Audit** tab.

Element	Description
Issue	Displays the issue location, which includes the file name and line number.

Element	**Description**
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>	Displays any custom tags if defined for the audit project. If the audit results have been submitted to Audit Assistant in Micro Focus Fortify Software Security Center, then in addition to any other custom tags, the tab displays the following tags: • **AA_Prediction**—Exploitability level that Audit Assistant assigned to the issue. You cannot modify this tag value. • **AA_Confidence**—Confidence level from Audit Assistant for the accuracy of its AA_Prediction value. This is a percentage, expressed in values that range from 0.000 to 1.000. For example, a value of 0.982 indicates a confidence level of 98.2 percent. You cannot modify this tag value. • **AA_Training**—Whether to include or exclude the issue from Audit Assistant training. You can modify this value. For more information about Audit Assistant, see the *Micro Focus Fortify Software Security Center User Guide*.
Suppress	Suppresses the issue.
File Bug	Provides access to a supported bug tracking system, such as Bugzilla or Azure DevOps Server. See the *Micro Focus Fortify Software System Requirements* document for a list of supported bug tracking systems.
Comments	Appends additional information about the issue as a comment.
Rule Information	Shows information, such as the category and kingdom that describes the issue.
More Information	Opens the **Details** tab.
Recommendations	Opens the **Recommendations** tab.

For information about auditing, see "Auditing Issues" on page 55.

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



Abstract:

Hardcoded passwords may compromise system security in a way that cannot be easily remedied.

Explanation:

It is never a good idea to hardcode a password. Not only does hardcoding a password allow all of the project's developers to view the password, it also makes fixing the problem extremely difficult. After the code is in production, the password cannot be changed without patching the software. If the account protected by the password is compromised, the owners of the system must choose between security and availability.

Example: The following code uses a hardcoded password to create a network credential:

```
...
NetworkCredential netCred =
        new NetworkCredential("scott", "tiger", domain);
```

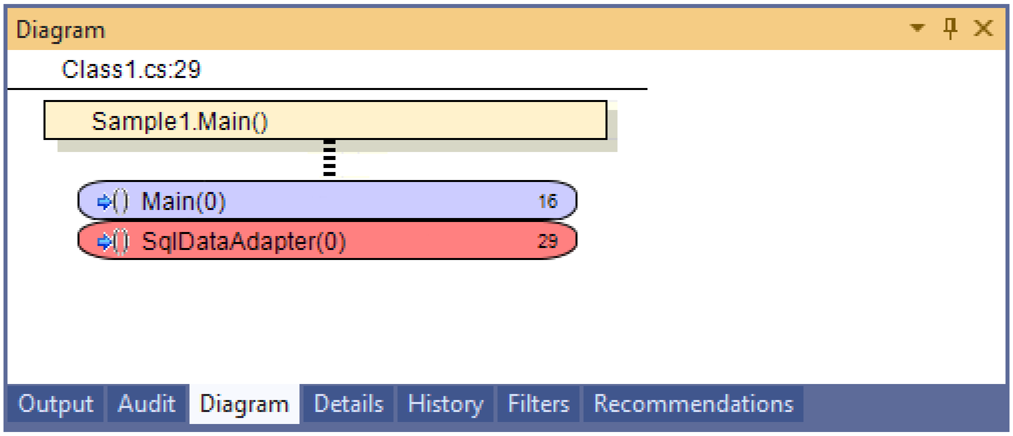
The Details tab includes some or all the sections described in the following table.

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

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

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

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

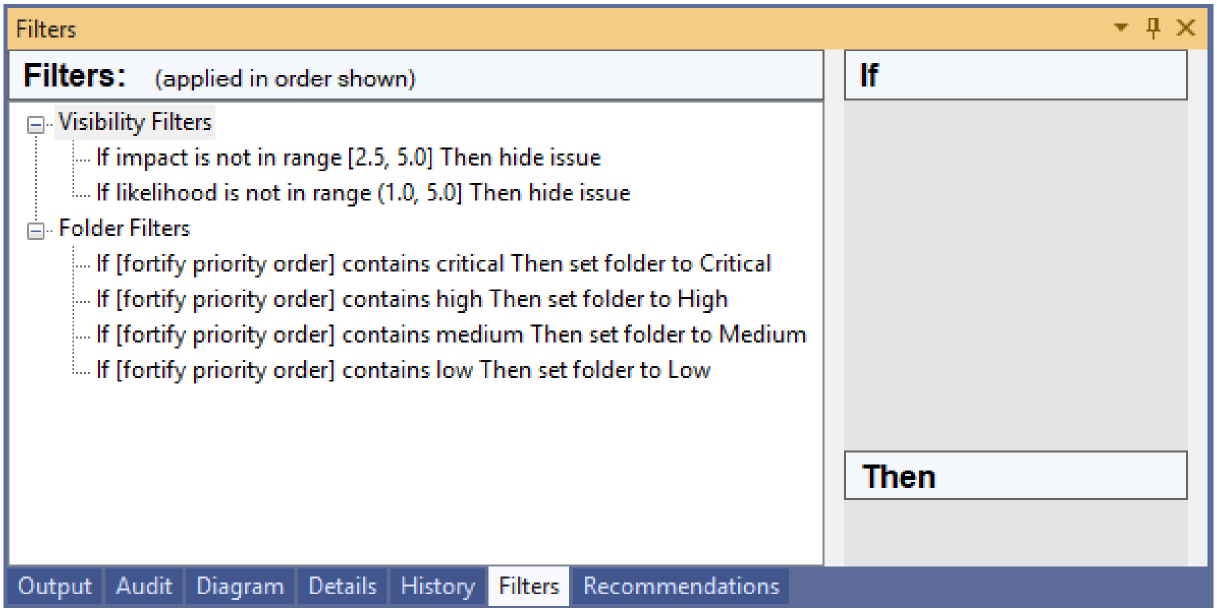


For dataflow issues, the trace starts with the first function to call the taint source, then traces the calls to the source (blue node) and ends the trace at the sink (red node). In the diagram, the source (src) and sink nodes are also labeled. A red X on a vertical axis indicates that the function called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

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

The icons used for the expression type of each node in the diagram are the same icons used in the Analysis Trace window. To see the icons and the descriptions, see "Analysis Trace Window" on page 36.

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



Visibility Filters
- If impact is not in range [2.5, 5.0] Then hide issue
- If likelihood is not in range (1.0, 5.0] Then hide issue

Folder Filters
- If [fortify priority order] contains critical Then set folder to Critical
- If [fortify priority order] contains high Then set folder to High
- If [fortify priority order] contains medium Then set folder to Medium
- If [fortify priority order] contains low Then set folder to Low

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

Element	Description
Filters	Displays a list of the visibility and folder filters configured in the selected filter set where: • **Visibility Filters** show or hide issues • **Folder Filters** sort the issues into the folder tabs in the Analysis Results window Right-click a filter to show issues that match the filter or to enable, disable, copy, or delete it.
If	Displays the conditions for the selected filter. The first list displays issue attributes, the second list specifies how to match the attribute, and the third list shows the value the filter matches.
Then	Displays the type of the selected filter, where **Hide Issue** is a visibility filter and **Set Folder to** is a folder filter.

For more information about creating filters, see "Creating a Filter from the Filters Tab" on page 62.

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 navigation tree vary according to which grouping option is selected in the Analysis Results window. The value you select from the **Group By** list sorts issues in all visible folders into subfolders.

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

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

Option	**Description**
Analysis	Groups issues by the audit analysis, such as Suspicious, Exploitable, and Not an Issue.
Analysis Type	Groups issues by analyzer product, such as SCA, WEBINSPECT, and SECURITYSCOPE (WebInspect Agent).
Analyzer	Groups issues by analyzer group, such as Control Flow, Data Flow, Semantic, and Structural.
App Defender Protected	Groups issues by whether Application Defender can protect the vulnerability category.
Category	Groups issues by vulnerability category. This is the default setting.
Category Analyzer	A custom group that groups issues by category and then analyzer.
File Name	Groups issues by file name.
Fortify Priority Order	Groups issues as Critical, High, Medium, and Low based on the combined values of Micro Focus Fortify Static Code Analyzer impact and likelihood.
Kingdom	Groups issues by the Seven Pernicious Kingdoms classification.
New Issue	Shows which issues are new since the last scan. For example, if you run a new scan, any issues that are new display in the tree under the **New Issue** subfolder and the others are displayed in the **Existing Issue** subfolder. Issues not found in the latest scan are displayed in the **Removed** subfolder.

Option	Description
	Note: If you are remediating results from Fortify Software Security Center, these subfolders are named **NEW**, **UPDATED**, and **REMOVED**, respectively.
<*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).
Package	Groups issues by package or namespace. Does not appear for projects for which this option is not applicable, such as C projects.
Priority by Category	A custom group that groups issues by Fortify Priority Order and then by category.
Sink	Groups issues that share the same 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 grouping.
<Edit>	Use to create a custom grouping option. **Note:** This option is not available when you remediate an audit project on Micro Focus Fortify Software Security Center.

Creating a Custom Group By Option

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

To create a new Group By option:

1. From the **Group by** list, select **<Edit>**.

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

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

```
-Buffer Overflow [0/2]
--DataFlow [0/1]
----Main.cs:234
-+Semantic [0/1]
```

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

Searching for Issues

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

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

Comparison	**Description**
contains	Searches for a term without any qualifying delimiters
equals	Searches for an exact match if the term is wrapped in quotation marks (" ")
regex	Searches for values that match a Java-style regular expression delimited by a forward slash (/) Example, `/eas.+?/` **Note:** This search comparison is not available when you remediate audit results stored on Micro Focus Fortify Software Security Center.
number range	Searches for a range of numbers using the standard mathematical interval notation of parentheses and/or brackets to indicate whether the endpoints are excluded or included, respectively. Example: (2,4] indicates greater than two and less than or equal to four

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.

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

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

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

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

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

Modifier	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.
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. Micro Focus Fortify Static Code Analyzer calculates the confidence value based on the number of assumptions made in code analysis. The more assumptions made, the lower the confidence value.
<custom_tagname>	Searches for issues based on the value of the specified custom tag. You can search a list-type custom tag using a range of values. The values of a list-type custom tag are an enumerated list where the first value is 0, the second is 1, and so on. You can use the search syntax for a range of numbers to search for ranges of list-type custom tag values. For example, analysis:[0,2]

Modifier	Description
	returns the issues that have the values of the first three Analysis values, 0, 1, and 2 (Not an Issue, Reliability Issue, and Bad Practice). To search a date-type custom tag, specify the date in the format: yyyy-mm-dd.
`dynamic`	Searches for issues that have the specified dynamic hot spot ranking value.
`file`	Searches for issues where the primary location or sink node function call occurs in the specified file.
`[fortify priority order]`	Searches for issues that have a priority level that matches the specified priority determined by the Fortify analyzers. Valid values are `critical`, `high`, `medium`, and `low`, based on the expected *impact* and *likelihood* of exploitation. The impact value indicates the potential damage that might result if an issue is successfully exploited. The likelihood value is a combination of confidence, accuracy of the rule, and probability that and attacker can exploit the issue.
`historyuser`	Searches for issues that have audit data modified by the specified user.
`impact`	Searches for issues based on the impact value specified (0.1 through 5.0).
`[instance id]`	Searches for an issue based on the specified instance ID.
`[issue age]`	Searches for the issue age, which is `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).

Modifier	Description
`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.
`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. **Note:** This search modifier is not available when you remediate audit results that are stored on Micro Focus Fortify Software Security Center.
`severity (sev)`	Searches for issues based on the specified severity value (legacy

Modifier	Description
	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 48.
`sourceline`	Searches for dataflow issues having taint source entering the flow on the specified line. Also see "line" on the previous page.
`status`	Searches issues that have the status `reviewed`, `unreviewed`, or `under review`.
`suppressed`	Searches for suppressed issues.
`taint`	Searches for issues that have the specified taint flag.
`trace`	Searches for issues that have the specified string in the dataflow trace. **Note:** This search modifier is not available when you remediate audit results that are stored on Fortify Software Security Center.
`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. **Note:** This search modifier is not available when you remediate audit results that are stored on Fortify Software Security Center.
`tracenodeallpaths`	Searches for the specified value in all the steps of the analysis trace.

Modifier	Description
	Note: This search modifier is not available in the remediation plugin.
`url`	Searches for issues based on the specified URL.
`user`	Searches for issues assigned to the specified user.
`<custom_tagname>`	Searches for issues based on the value of the specified custom tag. You can search a list-type custom tag using a range of values. The values of a list-type custom tag are an enumerated list where the first value is 0, the second is 1, and so on. You can use the search syntax for a range of numbers to search for ranges of list-type custom tag values. For example, `analysis:[0,2]` returns the issues that have the values of the first three analysis values, `0`, `1`, and `2` (Not an Issue, Reliability Issue, and Bad Practice). To search a date-type custom tag, specify the date in the format: yyyy-mm-dd.
`<metadata_listname>`	Searches for issues based on the value of the specified metadata external list (for example, `[cwe top 25]` *`<year>`*, `[owasp top ten` *`<year>`*`]`, `[pci ssf` *`<version>`*`]`, `[stig` *`<version>`*`]`, and others).

Search Query Examples

Consider the following search query examples:

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

  `category:"privacy violation" source:getssn file:jsp`
- To search for all file names that contain `com/fortify/awb`, type the following:

  `file:com/fortify/awb`
- To search for all paths that contain traces with `mydbcode.sqlcleanse` as part of the name, type the following:

  `trace:mydbcode.sqlcleanse`
- To search for all paths that contain traces with `cleanse` as part of the name, type the following:

  `trace:cleanse`

- To search for all issues that contain `cleanse` as part of any modifier, type the following:

  `cleanse`
- To search for all suppressed vulnerabilities with `asdf` in the comments, type the following:

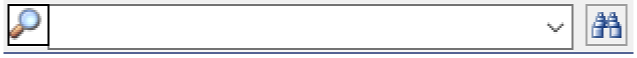
  `suppressed:true comments:asdf`
- To search for all categories except for SQL Injection, type the following:

  `category:!SQL Injection`

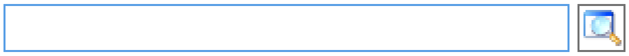
Performing Simple Searches

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

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

  When you remediate analysis results stored on Micro Focus Fortify Software Security Center, the search box appears as shown below:

  
- To select a search term you used previously (during the current session), click the arrow in the search box, and then select a search term from the list. Fortify Extension for Visual Studio discards saved search terms after you exit Visual Studio, saved.

  Note: Saved search terms are not available when you remediate audit results stored on Fortify Software Security Center.

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

Performing Advanced Searches

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

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

To use the advanced search feature:

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

   The Advanced Search dialog box opens.
2. From the first list on the left select a modifier.

   If you plan to specify an unqualified search term, select **Any Attribute** from the modifier list.
3. From the middle list, select a comparison term.
4. In the combo box on the right, either type a search term, or select one from the list.

   The search term list includes the known values in the current scan for the specified attribute. However, you can type any value into this field.
5. To add an AND or OR row to the query, click the **Add Criteria** icon.

6. To set the operator, click either **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 **Delete** ✕.
10. To remove all rows, at the bottom of the dialog box, click **Clear**.
11. To submit your completed search query, click **Find**.

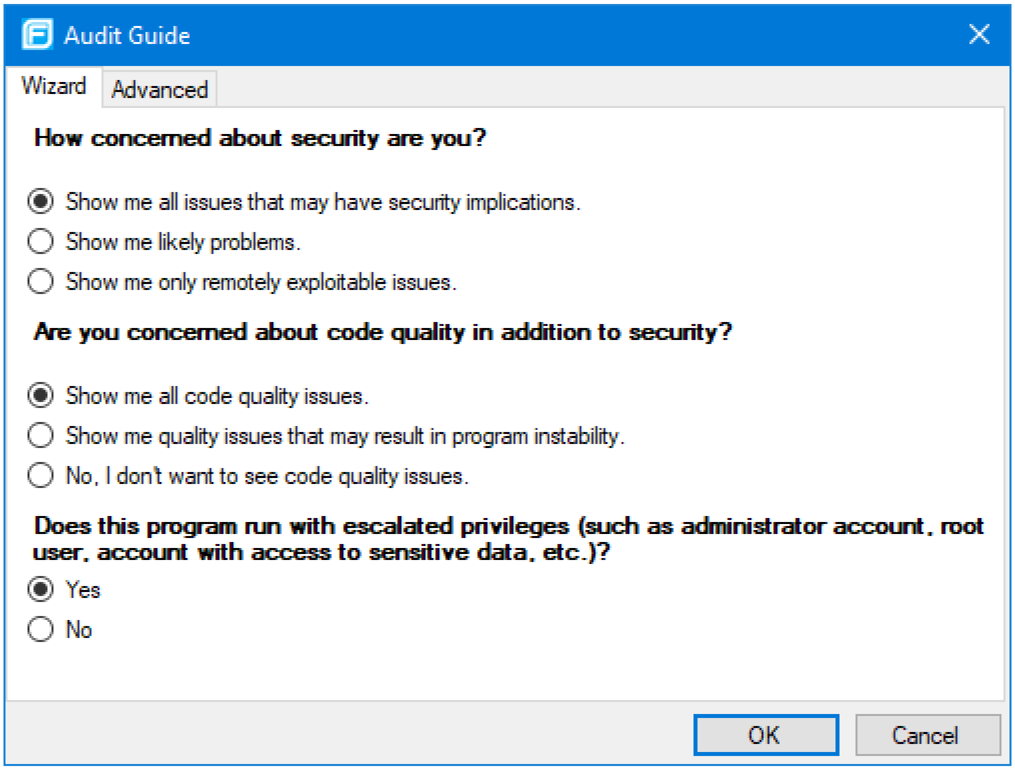
    > **Note: Find** is only enabled after you create a complete search query.

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**.



How concerned about security are you?

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

Are you concerned about code quality in addition to security?

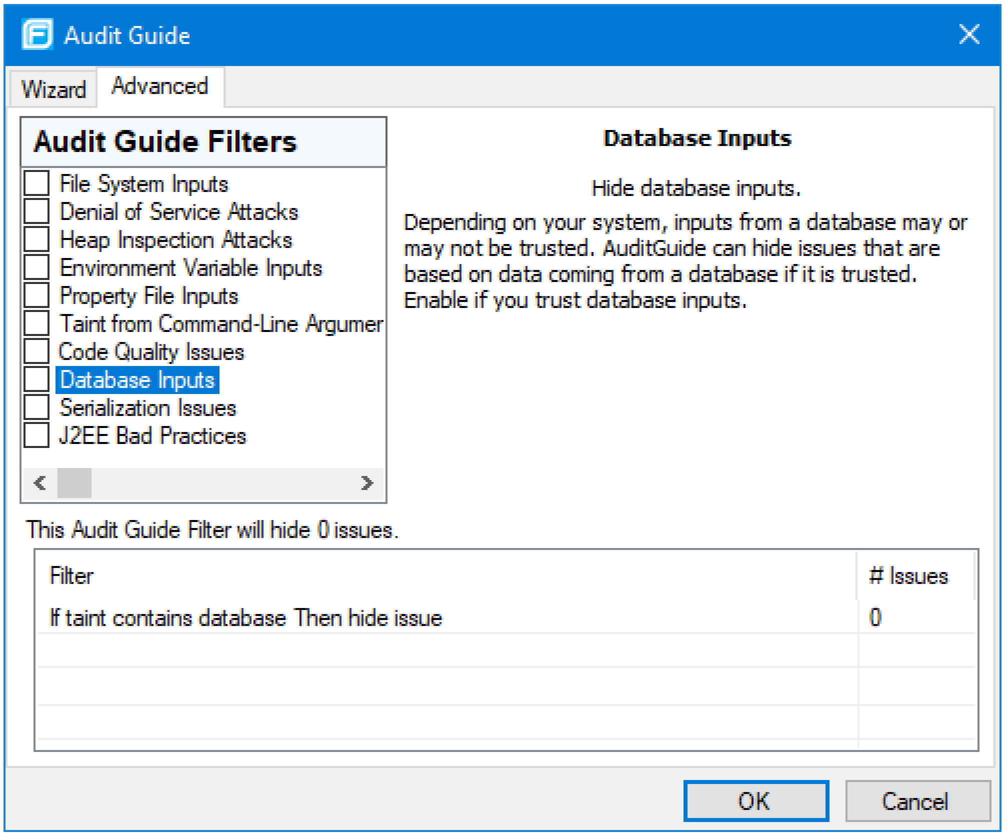
● Show me all code quality issues.
○ Show me quality issues that may result in program instability.
○ No, I don't want to see code quality issues.

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

● Yes
○ No

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

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



Audit Guide Filters

□ File System Inputs
□ Denial of Service Attacks
□ Heap Inspection Attacks
□ Environment Variable Inputs
□ Property File Inputs
□ Taint from Command-Line Argumer
□ Code Quality Issues
□ Database Inputs
□ Serialization Issues
□ J2EE Bad Practices

Database Inputs

Hide database inputs.

Depending on your system, inputs from a database may or may not be trusted. AuditGuide can hide issues that are based on data coming from a database if it is trusted. Enable if you trust database inputs.

This Audit Guide Filter will hide 0 issues.

Filter	# Issues
If taint contains database Then hide issue	0

- 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.

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

To refine your audit process, you can define your own custom tags. For example, you could create a custom tag to track the sign-off process for an issue. After a developer audits his own issues, a security expert can review those same issues and mark each as “approved” or “not approved.” For more information, see "Configuring Custom Tags for Auditing" on page 58.

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

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

Auditing Issues

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

1. Select the issue or group of issues in the Analysis Results window.

   For information about the Analysis Results window, see "Analysis Results Window" on page 33.
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 **More Information** link or the **Details** tab to get more details about the issue.
4. On the **Audit** tab, assign an **Analysis** value to the issue to represent your evaluation.
5. Specify values for any custom tags as required by your organization.

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

   > **Note:** If you select a different value for **Analysis** than the **AA_Prediction** value set by Audit Assistant, and you select Include from the **AA_Training** list, then the next time the data is submitted to Audit Assistant, it updates the information used to predict whether an issue represents a true vulnerability. For more information about Audit Assistant, see the *Micro Focus Fortify Software Security Center User Guide*.
7. (Optional) In the **Comments** box, add any comments relevant to the issue and your evaluation.

Suppressing Issues

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

To suppress an issue, do one of the following:

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

Viewing Suppressed Issues

To review results that have been suppressed:

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

Submitting an Issue as a Bug

You can submit issues to your bug tracking application if integration between the applications has been configured. See the *Micro Focus Fortify Software System Requirements* document for a list of supported client-side bug tracking plugins.

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 Bugtracker Integration dialog box opens. Select the bug tracking application, and then click **Select**.
3. Specify the values if changes are needed and review the issue description.

   Depending on the integration and your bug tracking application, the values include items such as product name, severity level, summary, and version.
4. Click **File Bug**.

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

Using Issue Templates

Micro Focus Fortify Static Code Analyzer produces comprehensive results for source code analysis. On large codebases, these results can be overwhelming. Issue templates provide features to sort and filter the results in ways that best suit your needs. The filtering and sorting mechanisms appropriate during a given phase in the development process can change depending on the phase of development. Similarly, the filtering and sorting mechanisms might vary depending on the role of the user.

You can sort issues by grouping issues into folders, which are logically defined sets of issues presented in the tabs on the Analysis Results window. You can further customize the sorting by providing custom definitions for the folders into which the issues are sorted. You can provide definitions for any number of folders, whose contents are then defined by filters. Filters can either alter the visibility of an issue or place it into a folder. When used to sort issues into folders, you can define the nature of the issues that appear in the customized folders.

You group filters into filter sets and then use the filter sets to sort and filter the issues displayed. An issue template can contain definitions for multiple filter sets. Using multiple filter sets in an audit project enables you to quickly change the sorting and visibility of the issues you are auditing. For example, the default issue template used in the interface provides two filter sets. These filter sets provide an increasingly restrictive view of security-related issues. Defining multiple filter sets for an audit project enables different 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 fields are displayed and the values for each

The issue template applied to a project uses the following order of preference:

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

Saving Issue Templates

Once an issue template is associated with an audit project, all changes made to that template, such as the addition of folders, custom tags, filter sets, or filters, apply to the audit project, and the issue template is stored in the FPR when the project is saved. For information about how to change the issue template associated with an audit project, see "Importing Issue Templates" on the next page.

Exporting Issue Templates

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

To export an issue template:

1. 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.

The filter sets and custom tags are updated.

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

Configuring Custom Tags for Auditing

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

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

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

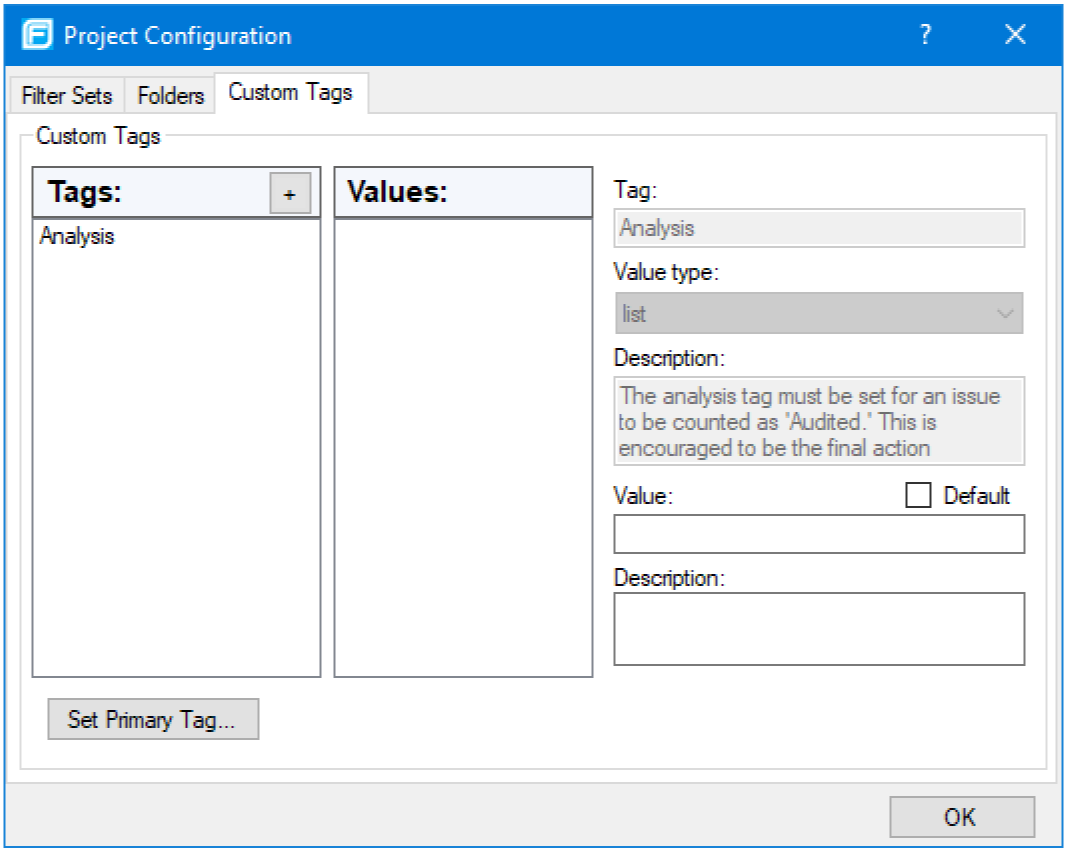
After you define a custom tag, the **Audit** tab displays it below the Analysis tag, which enables you to specify values as they relate to specific issues. The tag is also available in other areas of the interface, such as in the **Group By** list as a way to group issues in a folder, in the search field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

Adding a Custom Tag

You can 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.



Tags: Analysis

Tag: Analysis

Value type: list

Description: The analysis tag must be set for an issue to be counted as 'Audited.' This is encouraged to be the final action

Value: ☐ Default

Description:

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

   > **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 **Add Value** +.

   c. In the Add Value dialog box, type a value, and then click **OK**.

   d. To use this value as the default for the new tag, select a value in the **Values** list, and then select **Default** on the right.

   If no default is selected, the default value for the custom tag is empty.

   e. To add a description for the value, type it in the **Description** box.

   f. Repeat steps b through e until you have added all the tag values.

8. To add a description for any tag type:

   a. From the **Tags** list, select the tag.

   b. Type a description in the **Description** box on the right.

9. To make this custom tag the primary tag:

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

   a. Click **Set Primary Tag**.

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

   The primary tag determines the audit status for each issue as well as the audit icon in the **Analysis Results** view. 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 **Hide Tag** -.
5. Click **OK**.

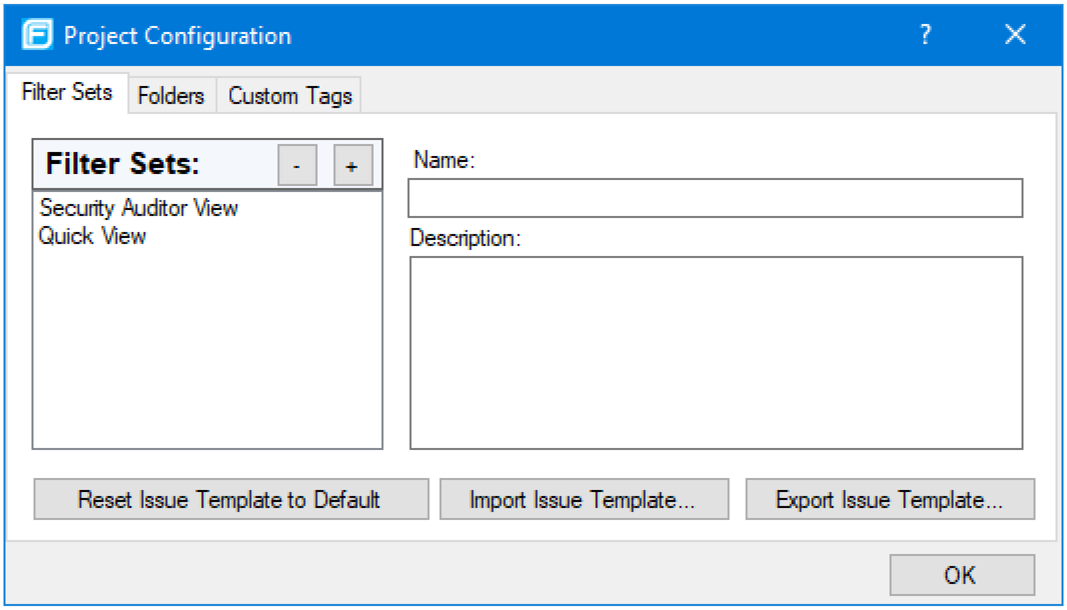
If you hide a tag that has an associated filter, you are prompted to delete the filter.

Creating a Filter Set

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

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

Creating a Filter from the Analysis Results Window

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

Note: To find the filter that directed the issue to the folder, right-click the issue, and select **Why is this issue here?** To find the filter that hid an issue, right-click the issue, and then select **Why is this issue hidden?**

To create a new filter from an issue:

1. In the Analysis Results window, select a filter set from the **Filter Set** list.
2. Right-click an issue, and then select **Generate Filter**.

   The Create Filter dialog box opens and displays a list of suggested conditions.
3. To expand the conditions list, click **More Choices**.
4. Select the conditions to use in the filter. You can fine tune the filter later from the **Filter** tab.
5. To specify the type of filter you want to create, do one of the following:
   - To create a visibility filter, select **Hide Issue**.
   - To create a folder filter, select **Set Folder to**, and then select the folder name or select **Create New** to create a new folder.

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

   The new filter is placed at the end of the filter list. For folder filters, this gives the new filter the highest priority. Issues matching the new folder filter appear in the targeted folder.
7. To change the priority of a folder filter, drag the filter higher in the folder filter list.

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

Creating a Filter from the Filters Tab

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

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

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

1. From the **Filter Set** list, select a filter set.
2. Right-click **Visibility Filters** or **Folder Filters**, and then select **Create New Filter**.
3. From the first list, select an issue attribute.
4. From the second list, select a value to specify how to match the value.

   The third list automatically displays the attribute values.
5. From the third list, select a value or specify a range as instructed in the **If** line.
6. Set **Then** to one of the following options:
   - To create a visibility filter, select **Hide Issue**.
   - To create a folder filter, select **Set Folder to**, and then select the folder name or select **Create New** to create a new folder.

   The new filter displays at the end of the list. For folder filters, this gives the new filter the highest priority. Issues that match the new folder filter are displayed in the targeted folder.
7. To change the priority, drag the filter higher in the folder filter list.

The issues are sorted based on the new filter.

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

Copying a Filter to Another Filter Set

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

To copy a filter:

1. From the **Filter Set** list, select a filter set.
2. On the **Filters** tab, right-click a filter, and then select **Copy Filter To**.

   The Select a Filter Set dialog box lists the filter sets.
3. Select a filter set, and then click **OK**.

   The filter is added to the destination filter set in the last position.
4. To change the order of the folder filters, drag and drop the filters in the list.

Managing Folders

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

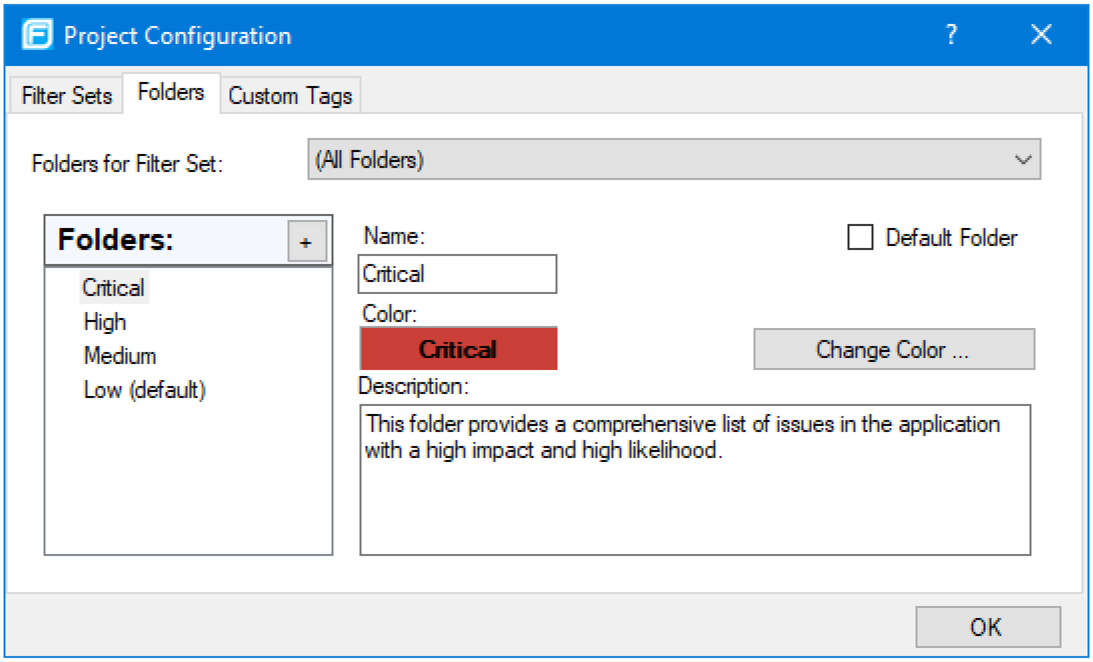
Creating a Folder

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

To create a folder:

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

   Currently defined folders are listed on the left. Fields that indicate the name, color, and description of the selected folder are on the right.



Folders for Filter Set: (All Folders)

Folders:

- Critical
- High
- Medium
- Low (default)

Name: Critical

☐ Default Folder

Color: Critical

Description: This folder provides a comprehensive list of issues in the application with a high impact and high likelihood.

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

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

4. To add a folder:

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

      The Create New Folder dialog box opens.

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

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

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

6. Click **OK**.

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

> **Note:** To display issues in this folder, create a folder filter that targets the new folder (see "Creating a Filter from the Analysis Results Window" on page 61 and "Creating a Filter from the Filters Tab" on page 62).

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 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. Select the folder in the **Folders** list.

   The folder properties are displayed on the right.
5. In the **Name** box, type the new folder name.
6. Click **OK**.

The tab displays the new folder name.

Removing a Folder

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

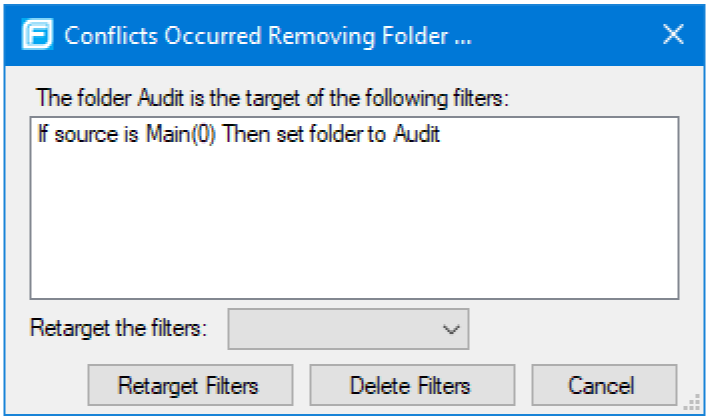
To remove a folder:

1. 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 contains the folder you want to remove.

   The folders in the selected filter set are listed.
4. Next to **Folders**, select the folder, and then click **-**.

   The folder is removed only from the selected filter set.

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



The folder Audit is the target of the following filters:

If source is Main(0) Then set folder to Audit

Retarget the filters:

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.

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

The folder is no longer displayed as a tab.

Generating Analysis Results Reports

The following topics provide information about generating BIRT and legacy reports for your analysis results.

BIRT Reports

You can generate BIRT reports from Fortify Extension for Visual Studio or from the command line (BIRTReportGenerator utility). For information on how to generate BIRT reports from the command line, see the *Micro Focus Fortify Static Code Analyzer User Guide*.

The following table describes the BIRT reports available.

Report Template	Description
CWE Top 25	This report lists the most widespread and critical weaknesses that can lead to serious software vulnerabilities (based on the National Vulnerability Database).
CWE/SANS Top 25	This report details issues related to the CWE/SANS Top 25 Most Dangerous Programming Errors and provides information about where and how to fix the issues. It describes the technical risk posed by unremediated issues discovered during analysis and provides an estimate of the development effort needed to test, verify, and fix them.

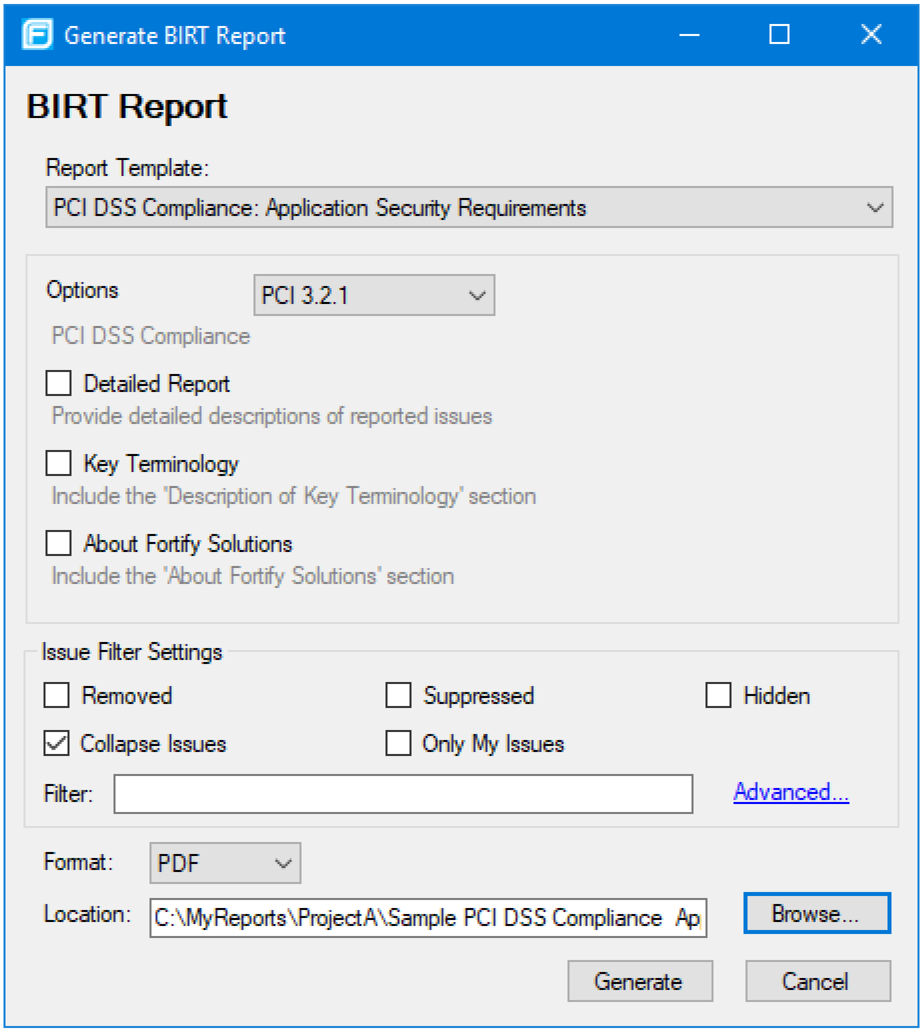
Report Template	Description
Developer Workbook	This report provides the information a developer needs to understand and fix the issues discovered during an application audit.
DISA CCI 2	This report provides a standard identifier for policy-based requirements that connects high-level policy expressions 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 an provides an estimate of the development effort needed to test, verify, and fix them.
OWASP ASVS 4.0	This report groups detected issues based the OWASP Application Security Verification Standard security requirements for secure development.
OWASP Mobile Top 10	This report details the top ten OWASP mobile-related issues and provides information about where and how to fix them. It describes the technical risk posed by the unremediated issues discovered during analysis and gives an estimate of the development effort required to test, verify, and fix them.

Report Template	**Description**
OWASP Top 10	This report details the top ten OWASP-related issues and provides information about where and how to fix them. It describes the technical risks posed by unremediated issues discovered during analysis and gives an estimate of the development effort required to test, verify, and fix the issues.
PCI DSS Compliance: Application Security Requirements	This report summarizes the application security portions of PCI DSS. It includes tests for 21 application security-related requirements across sections 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is either “In Place” or “Not In Place.”
PCI SSF Compliance: Secure Software Requirements	This report summarizes the application security portions of PCI SSF v1.0. 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 BIRT Reports

To generate a report:

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



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:

Format: PDF

Location: C:\MyReports\ProjectA\Sample PCI DSS Compliance Ap

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:
   - Click **Removed** to include removed issues in the report.
   - Click **Suppressed** to include suppressed issues in the report.

- Click **Hidden** to include hidden issues in the report.
- Click **Collapse Issues** to collapse issues of the same sink and type into a single issue.
- Click **Only My Issues** to include only issues assigned to your user name.
- Click **Advanced** to build a search query to further filter the issues to include in the report. For more information about the search modifiers, see "Search Modifiers" on page 46.

6. From the **Format** list, select a format for the report (PDF, HTML, DOC, or XLS).

   > **Note:** When you open the XLS file in Excel, you might get a warning that the file format and the file extension do not match. You can safely open the file in Excel.

7. To specify an alternate location to save the report, click **Browse** and select a location.
8. Click **Generate**.
9. If a report with the same file name already exists, you are prompted to either:
   - Click **No** to overwrite the existing report.
   - Click **Yes** to have the report saved to a file with a sequential number appended to the file name (for example: `Sample1_DISA_STIG(1).pdf`).

About Legacy Reports

The legacy reports include user-configurable report templates. Report templates provide several optional sections and subsections that gather and present specific types of data. You can generate legacy reports from Fortify Extension for Visual Studio or from the command line (ReportGenerator utility). For information on how to generate legacy reports from the command line, see the *Micro Focus Fortify Static Code Analyzer 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 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 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**.

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 75). 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 on the analysis performed and the high-level details of the audit that was performed. It also provides a high-level description and examples of categories that are of the highest priority.
- **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 Micro Focus Fortify Static Code Analyzer 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 on the left side.
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: `<relative_file_path> # Lines # kb <timestamp>`
$FILTERSET_DETAILS$	List of filters used by the current filter set
$FILTERSET_NAME$	Name of the current filter set
$FORTIFY_SCA_ VERSION$	Micro Focus Fortify Static Code Analyzer version
$LIBDIR_LISTING$	Libdirs specified during scan, one relative path per line
$LOC$	Total lines of code
$NUMBER_OF_FILES$	Total number of files scanned
$PROJECT_BUILD_	Build label of project

Variable	Description
LABEL$	
$PROJECT_NAME$	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 Fortify Static Code Analyzer `-build-label` option was used in the scan)
$WARNINGS$	Complete list of warnings issued (same format as project summary)
$WARNING_ SUMMARY$	Number of warnings found in 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 45.

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 45.
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 `<sca_install_dir>\Core\config\reports`.

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

Adding Legacy Report Sections

You can add report sections by editing the XML files. In the structure of the XML, the `ReportSection` 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:

```
<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 72. 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 Micro Focus 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 directory, and then click **OK**.

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

About Merging Audit Data

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

> **Note:** Issues are not merged. Only the newer scanned issues are shown. Issues in the older file that are not in the newer file are marked as removed.

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

Merging Audit Data

To merge audit projects:

1. Open an audit project in Visual Studio.
2. 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 on Micro Focus Fortify Software Security Center collaboratively with other Fortify Software Security Center users.

To start a collaborative audit:

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

      The Fortify Software Security Center URL includes both the port number and the context path `/ssc`. For example, `http://my.domain.com:8080/ssc`.

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

d. Click **OK**.

2. From the Fortify extension menu, select **Open Collaborative Audit**.

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

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 17.

4. In the Download Collaborative Audit dialog box, select an application version, and then click **Select**.

   The Fortify Extension for Visual Studio downloads the audit project file from Fortify Software Security Center and opens it in the auditing interface.

5. Audit the project as described in "Auditing Issues" on page 55.

6. When you have completed 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 Micro Focus 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, Micro Focus 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 uploaded audit projects scanned in quick scan mode are processed. For more information, see analysis results processing rules in the *Micro Focus Fortify Software Security Center User Guide*.

To upload results to Micro Focus 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 panel, select **Server Configuration**.

   c. Under **Software Security Center**, specify the **Server URL** for Fortify Software Security Center.

      The Fortify Software Security Center URL includes both the port number and the context path `/ssc`. For example, `http://my.domain.com:8080/ssc`.

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

   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 17.

   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.

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. See the *Micro Focus Fortify Software System Requirements* document for the supported versions.

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

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

Locating the Log Files

To get assistance in diagnosing an issue, send the log files to Micro Focus Fortify Customer Support. On Windows systems, the log files are in the following directories:

- `C:\users\<username>\AppData\Local\Fortify\sca<version>\log`
  This log file is only available if you analyze the code with Micro Focus Fortify Static Code Analyzer.
- `C:\users\<username>\AppData\Local\Fortify\VS<VSversion>-<version>\log`
- `C:\users\<username>\AppData\Local\Fortify\scancentral-<version>\log`
  This log file is only available if you analyze the code with Micro Focus Fortify ScanCentral SAST.

Chapter 3: Remediating Results from Fortify Software Security Center

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

This section contains the following topics:

Working with Applications

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

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

Filters determine which issues are visible in the user interface. The filters are organized into filter sets. An issue template can contain definitions for multiple filter sets. Using multiple filter sets in an audit project enables you to quickly change the sorting and visibility of issues.

Connecting to a Fortify Software Security Center Application

To select an application on Fortify Software Security Center:

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 panel, select **Server Configuration**.
   c. Under **Software Security Center**, specify the **Server URL** for Fortify Software Security Center.

      The Fortify Software Security Center URL includes both the port number and the context path `/ssc`. For example, `http://my.domain.com:8080/ssc`.

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

   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 17.

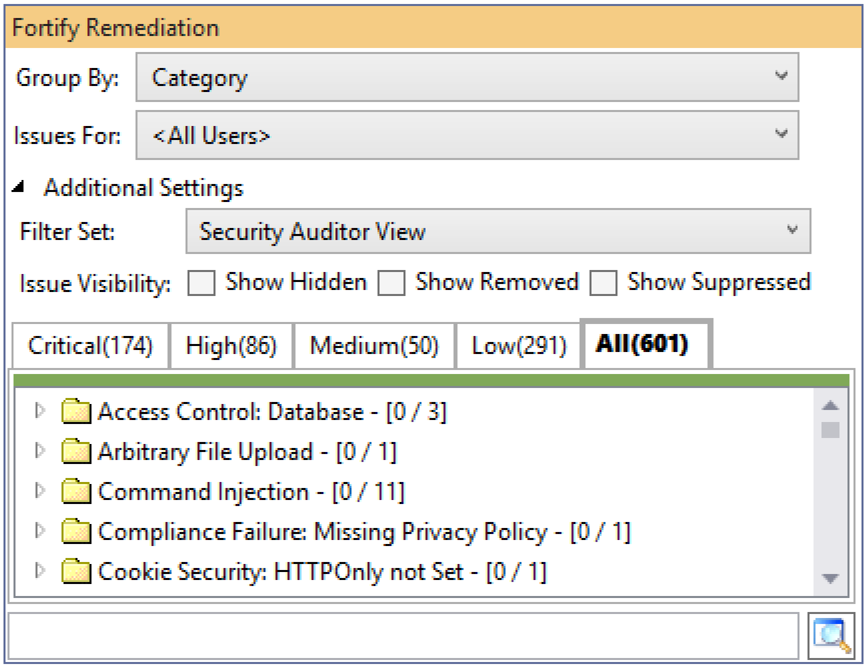
4. In the Select Application Version dialog box, select the application version you want to open, and then click **OK**.

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

Viewing and Selecting Issues in an Application

When you connect to a Micro Focus Fortify Software Security Center application, the Fortify Extension for Visual Studio downloads the issues for that application version. Fortify Software Security Center provides several default folder types. Your view might be different, depending on whether your organization has created custom folders.

1. In the Fortify Remediation view, expand the **Additional Settings** section to access the filter and issue visibility settings.



Fortify Remediation

Group By: Category

Issues For: <All Users>

Additional Settings

Filter Set: Security Auditor View

Issue Visibility: □ Show Hidden □ Show Removed □ Show Suppressed

Critical(174) | High(86) | Medium(50) | Low(291) | **All(601)**

- Access Control: Database - [0 / 3]
- Arbitrary File Upload - [0 / 1]
- Command Injection - [0 / 11]
- Compliance Failure: Missing Privacy Policy - [0 / 1]
- Cookie Security: HTTPOnly not Set - [0 / 1]

2. 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.

3. From the **Group By** list, select a value to use to sort issues in all visible folders into groups.

The default grouping is **Category**. For a description of the **Group By** options, see "Grouping Issues" on page 43.

4. From the **Issues For** list, select one of the following:
   - **<All Users>**
   - Your Fortify Software Security Center user name. This is the default.
5. Click one of the following category tabs (folders).
   - The **Critical** tab contains issues that have a high impact and a high likelihood of exploitation. Fortify recommends that you remediate critical issues immediately.
   - The **High** tab contains issues that have a high impact and a low likelihood of exploitation. Fortify recommends that you remediate high issues with the next patch release.
   - The **Medium** tab contains issues that a have low impact and a high likelihood of exploitation. Fortify recommends that you remediate medium issues as time permits.
   - The **Low** tab contains issues that have a low impact and a low likelihood of exploitation. Fortify recommends that you remediate low issues as time permits (your organization can customize this category).
   - The **All** tab contains all issues.

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

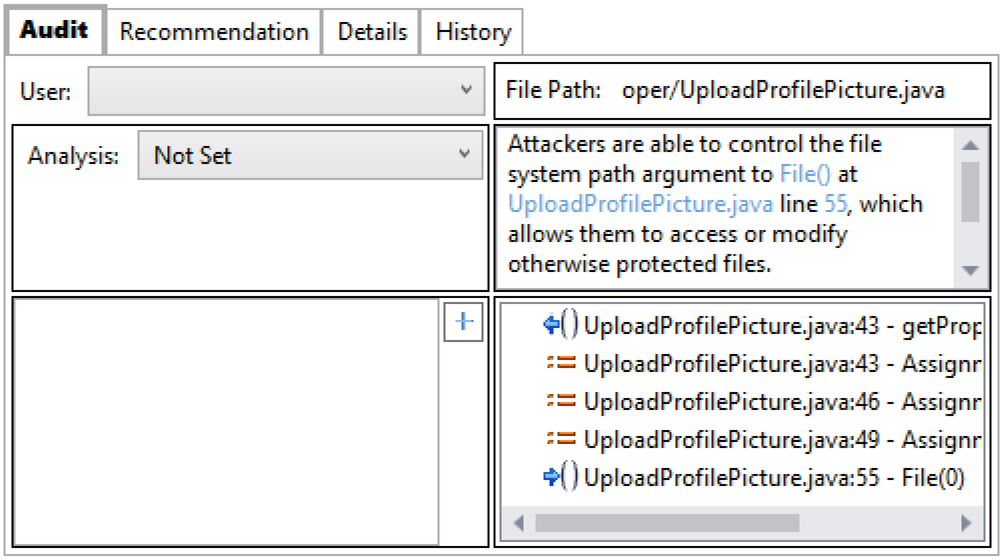
Working with Issues

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

This section provides descriptions of these tabs and their components.

Audit Tab

The **Audit** tab provides a dashboard for issues.



User:

File Path: oper/UploadProfilePicture.java

Analysis: Not Set

Attackers are able to control the file system path argument to File() at UploadProfilePicture.java line 55, which allows them to access or modify otherwise protected files.

```
UploadProfilePicture.java:43 - getProp
UploadProfilePicture.java:43 - Assignr
UploadProfilePicture.java:46 - Assignr
UploadProfilePicture.java:49 - Assignr
UploadProfilePicture.java:55 - File(0)
```

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

Element	**Description**
User	Select a name from this list to assign a user to the selected issue.
Analysis	Displays the analysis type for the selected issue. To change the analysis type, select an item from the list.
<custom_tagname>	Any custom tags your organization has defined in Micro Focus Fortify Software Security Center. If available, these are displayed below the Analysis list. If the audit results have been submitted to Audit Assistant in Fortify Software Security Center, then in addition to any other custom tags, the tab displays the following tags: • **AA_Prediction**—Exploitability level that Audit Assistant assigned to the issue. You cannot modify this tag value. • **AA_Confidence**—Confidence level from Audit Assistant for the accuracy of its AA_Prediction value. This is a percentage, expressed in values that range from 0.000 to 1.000. For example, a value of 0.982 indicates a confidence level of 98.2 percent. You cannot modify this tag value. • **AA_Training**—Whether to include or exclude the issue from Audit

Element	Description
	Assistant training. You can modify this value. For more information about Audit Assistant, see the *Micro Focus Fortify Software Security Center User Guide*.
File Path (top right)	The path to the location of the source file for the selected issue.
Issue Abstract (below File Path)	Displays a summary of the selected issue.
Analysis Trace (bottom right)	Lists 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 36.
Comments (bottom left)	Displays any comments added to the issue. To add a comment to the selected issue: 1. Click **Add Comment** ＋. 2. Type a comment, and then click **OK**.

Recommendation Tab

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

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

Details Tab

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

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

History Tab

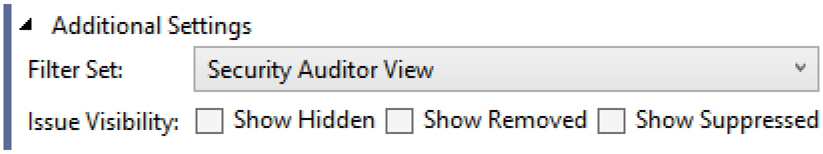
The **History** tab shows a history of audit actions, including details such as the time and date, and the name of the user who modified the issue.

Customizing Issue Visibility

You can customize the Fortify Remediation window to determine which issues it displays. You can specify issue visibility from the Fortify Remediation window.

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

1. In the Fortify Remediation window, expand the **Additional Settings** section.



Additional Settings

Filter Set: Security Auditor View

Issue Visibility: □ Show Hidden □ Show Removed □ Show Suppressed

2. Select or clear the following check boxes:
   - 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**.

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

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

The Fortify Remediation window displays issues based on your selection.

Note: You can also change 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

You can use the search box below the issues list in the **Analysis Results** window to search for issues. For detailed instructions about the search capabilities, see "Searching for Issues" on page 45.

Assigning Users to Issues

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

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

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

Assigning Tags to Issues

To assign tag values to an issue:

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

   For text- and decimal-type custom tags, type the value in the field, and then click **Save** (💾). Text-type custom tags accept up to 500 characters (HTML/XML tags and newlines are not allowed).

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

Locating Issues in Source Code

Because the Fortify Extension for Visual Studio works as an extension to your Visual Studio IDE, you can use it to locate security-related issues in your code. The project you have open in Visual Studio must match the project (application and application version) you opened in the Fortify Extension for Visual Studio from Fortify Software Security Center.

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

- From the issues list in the Fortify Remediation window, select an issue.
- From the **Audit** tab, select an issue from the Analysis Trace list.

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

Send Documentation Feedback

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

> **Note:** If you are experiencing a technical issue with our product, do not email the documentation team. Instead, contact Micro Focus Fortify 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 21.1.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!