Micro Focus
Fortify Security Assistant Extension for Visual Studio

Software Version: 18.10

User Guide

Document Release Date: May 2018
Software Release Date: May 2018

MICRO FOCUS®

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

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

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

Contents

Preface

Contacting Micro Focus Fortify Customer Support

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

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

https://softwaresupport.softwaregrp.com

To Call Support

1.844.260.7219

For More Information

For more information about Fortify software products:
https://software.microfocus.com/solutions/application-security

About the Documentation Set

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

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

Chapter 1: Introduction

This section contains the following topics:

Fortify Security Assistant Extension for Visual Studio

Fortify Security Assistant Extension for Visual Studio (Fortify Security Assistant) works with a portion of the Fortify security content to provide alerts to potential security issues as you write your code. Fortify Security Assistant can detect issues in C# (`.cs`), Razor (`.cshtml`), WebForms (`.aspx`), and `.config`, `.xml`, and `.ini` files.

Fortify Security Assistant provides detailed information about security risks and recommendations for how to secure the potential issue. Fortify Security Assistant includes both structural and configuration analyzers to detect:

- Potentially dangerous uses of functions and APIs
- Insecure application configuration

Fortify Security Content

Fortify Security Assistant uses a knowledge base of rules to enforce secure coding standards applicable to the codebase for static analysis. Micro Focus Fortify Software Security Content consists of Fortify Secure Coding Rulepacks, which describe general secure coding idioms for popular languages and public APIs.

Fortify Security Assistant Requirements

Fortify Security Assistant requires:

- A valid Fortify license file to scan for issues
- Up-to-date Micro Focus Fortify Software Security Content

For information about how to obtain a Fortify license, contact Micro Focus Fortify Customer Support. You can download the Fortify Security Content directly from Fortify Security Assistant or you can use a local copy if you do not have a network connection to the Fortify Customer Portal. For instructions, see .

Fortify Security Assistant requires the software packages listed in the following table.

Software	Version
Visual Studio 2017 Community, Professional, and Enterprise	15.6 or later
.NET Framework	4.6.1 or later

Chapter 2: Installation and Configuration

This section contains the following topics:

Installing Fortify Security Assistant

Note: These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.
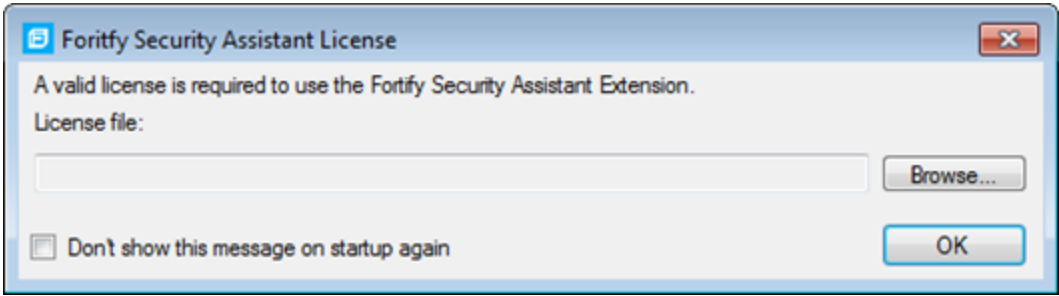
To install the Fortify Security Assistant Visual Studio extension:

1. In Visual Studio, select **Tools > Extensions and Updates**.
2. Search the Visual Studio Marketplace for `Fortify Security Assistant`.
3. Download and install the Fortify Security Assistant Extension for Visual Studio.

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

The menu bar now includes the **Fortify Security Assistant** menu.

The first time you install the extension, you are prompted to provide a license file and Micro Focus Fortify Software Security Content. Alternatively, you can specify this information later (see "Configuring Fortify Security Assistant" on page 9).

The license for Fortify Security Assistant expires annually. You do not need to specify the Fortify license file again until the license expires.

After you specify the Fortify license, you are prompted to update Fortify Security Content.
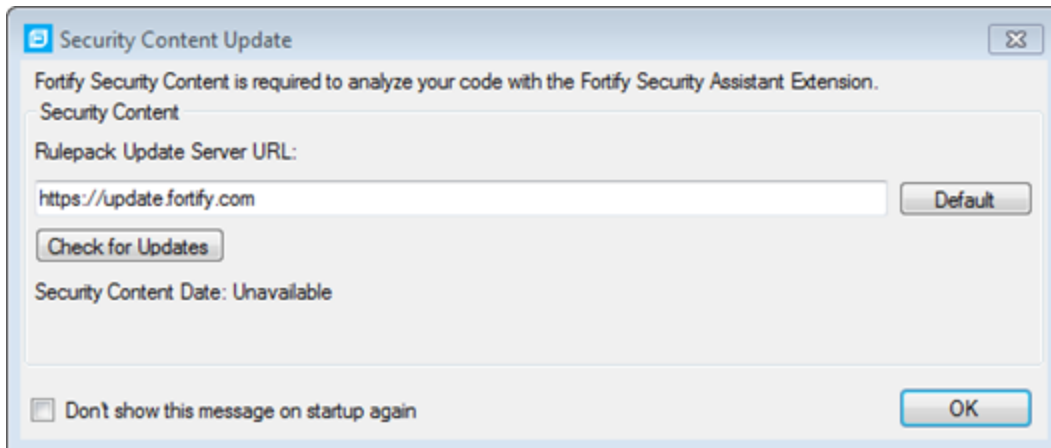
To specify the Fortify Security Content, you can either:

- Click **Check for Updates** to download the Fortify Security Content directly from the specified **Rulepack update server URL**.

    Note: If you get an error that indicates the downloaded security content is unverified, you might have an invalid license file. Contact Micro Focus Fortify Customer Support for assistance.

- Click **OK** if you do not have a network connection to the Fortify Customer Portal and you want to use a local copy of Fortify Security Content. For instructions, see "Using Fortify Security Content from a Local Package" below).

Using Fortify Security Content from a Local Package

If you do not have a network connection to the Fortify Customer Portal, Fortify Security Assistant can use the Fortify Security Content from a local copy. The file must be named `rulePacks.zip`.

To configure Fortify Security Assistant to use Fortify Security Content from a local package:

1. Navigate to `C:\Users\<username>\AppData\Local\Fortify\SecurityAssistantVS-<version>`.
2. Place the Fortify Security Content file `rulePacks.zip` in this folder.
3. Restart Visual Studio.

Configuring Fortify Security Assistant

To scan projects or solutions, you must have a valid Fortify license file and up-to-date Micro Focus Fortify Software Security Content. To download security content from the Fortify Customer Portal, you must be connected to the Internet and have your network connections configured to access the Fortify Customer Portal (https://update.fortify.com). To update Fortify Software Security Content from a local file, see "Using Fortify Security Content from a Local Package" on the previous page.

To configure Fortify Security Assistant:

1. From the Visual Studio menu bar, select **Fortify Security Assistant > Options**.
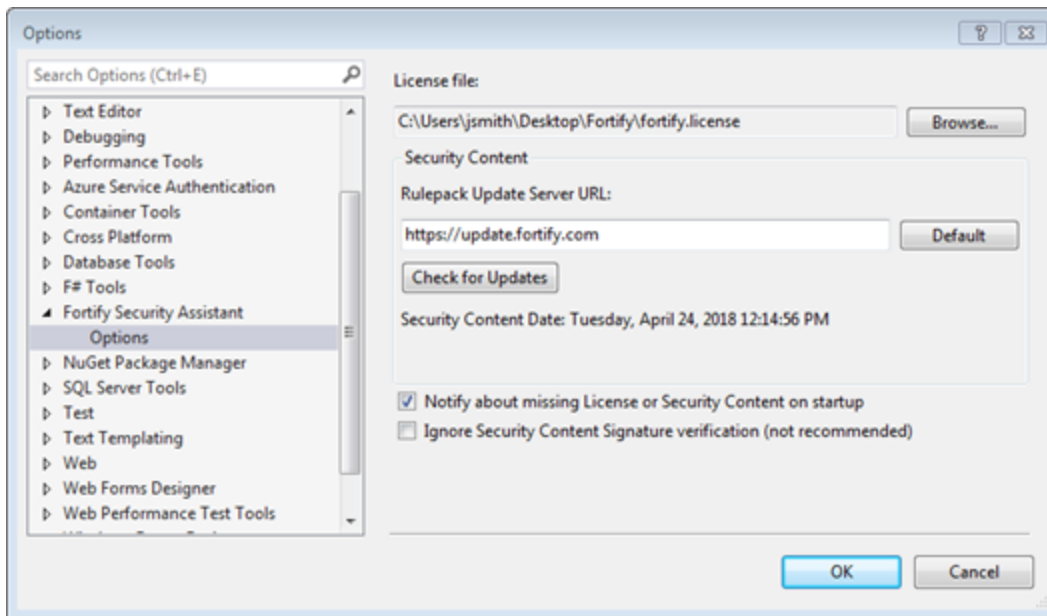
2. To specify the license file, click **Browse** next to the **License File** box and navigate to the license file on your system.

3. To update security content:

   a. In the **Rulepack Update Server URL** box, type a Rulepack update server URL.

      If you want to obtain the Fortify Security Content from a URL other than the Fortify Customer Portal, you must have a public key so that Fortify Security Assistant can verify the security content. Place the public key in the
      `C:\Users\`*`<username>`*`\AppData\Local\Fortify\SecurityAssistantVS-`*`<version>`*`/keys` directory. You can bypass the Fortify Security Content verification by selecting **Ignore Security Content Signature verification**.

      Note: Click **Default** to set the URL to the Fortify Customer Portal.

   b. Click **Check for Updates**.

      Note: If you get an error that indicates the downloaded security content is unverified, you might have an invalid license file. Contact Micro Focus Fortify Customer Support for

> assistance.

4. Click **OK**.

Fortify Security Assistant re-inspects the solution to refresh any issues reported so that it matches your configuration settings.

Uninstalling Fortify Security Assistant

Note: These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.

To uninstall the Fortify Security Assistant Visual Studio extension:

1. In Visual Studio, select **Tools > Extensions and Updates**.
2. Select **Fortify Security Assistant for Visual Studio**, and then click **Uninstall**.
3. Click **Yes** to confirm the pending uninstallation.

Chapter 3: Using Fortify Security Assistant

Fortify Security Assistant Extension for Visual Studio notifies you of any detected issues as you write your code. You can also have Fortify Security Assistant Extension for Visual Studio examine an entire solution and then you can review possible security issues (see "Scanning Solutions for Issues" on the next page).

This section contains the following topics:

Finding Security Issues as you Write Code

As you write your code, Fortify Security Assistant provides notifications of potential security issues.

To review the security issues:

- Fortify Security Assistant highlights possible security issues in the code. Pause your cursor over the highlighted code to open a tooltip that briefly describes the issue as shown in the following example:

```
<authentication mode="Forms">
  <forms name="customer_login" timeout="10"  requireSSL="false"
         The application session cookie is created without the secure flag set to true.
    <user name="admin" password="admin" />
    <user name="mario" password="luigi" />
    <user name="bob" password="password" />
  </credentials>
  </forms>
</authentication>
```

- Click the issue description in the tooltip to see a detailed description of it in the **Vulnerability Details** window.
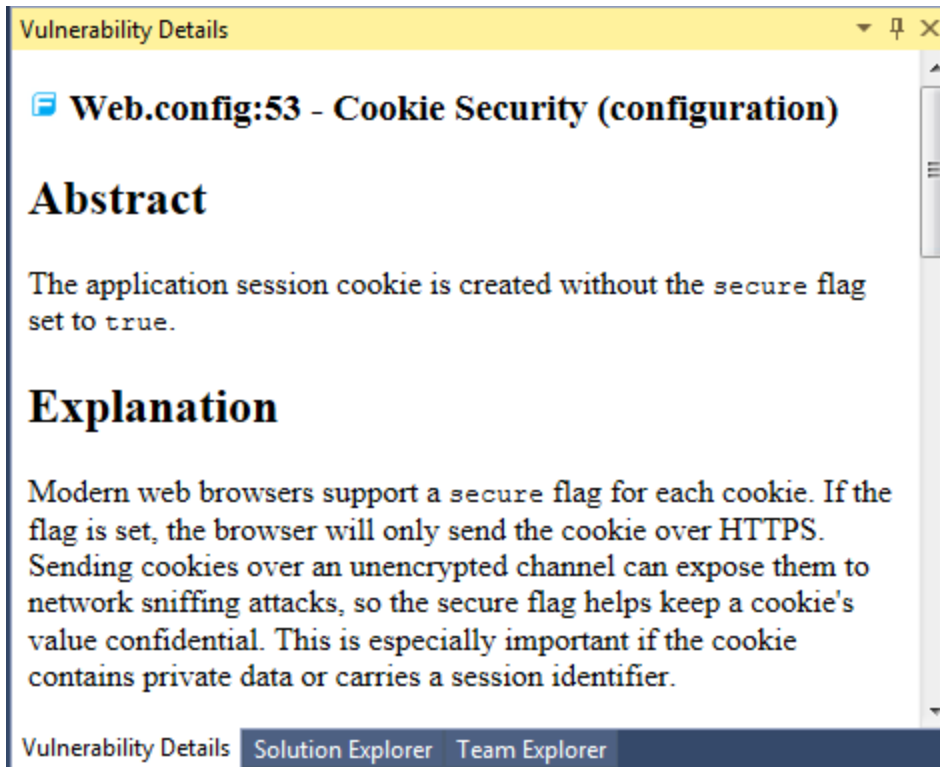
- You can also see any issues detected in the **Error List** window.

  For more information about reviewing the issues in the **Error List** window, see "Working with Security Assistant Issues in the Error List" on the next page.

Scanning Solutions for Issues

You can use Fortify Security Assistant to analyze a solution and identify security issues. You cannot make any code changes during the analysis.

To scan a solution for issues:

1. Select **Fortify Security Assistant > Analyze Solution**.

   You can cancel at any time.

   > **Note:** If you cancel the analysis, any Issues detected in projects that completed before the cancellation are shown in the **Error List** window.

2. When the analysis is complete, click **Close**.

Fortify Security Assistant displays any possible issues detected in the **Error List** window. For information about reviewing the security issues in this window, see "Working with Security Assistant Issues in the Error List" on the next page.

Working with Security Assistant Issues in the Error List

Fortify Security Assistant displays all the detected security issues for the code that has been analyzed in the **Error List** window's **Warnings** tab.

To see a detailed description of an issue, right-click the issue, and then select **View Vulnerability Details**. The **Vulnerability Details** window opens and provides an explanation of the issue and recommendations for how to fix the issue.

> **Note:** If the **Vulnerability Details** window is already open, click an issue to see the corresponding details in this window.

To locate the line of code where the issue was found, double-click the issue.
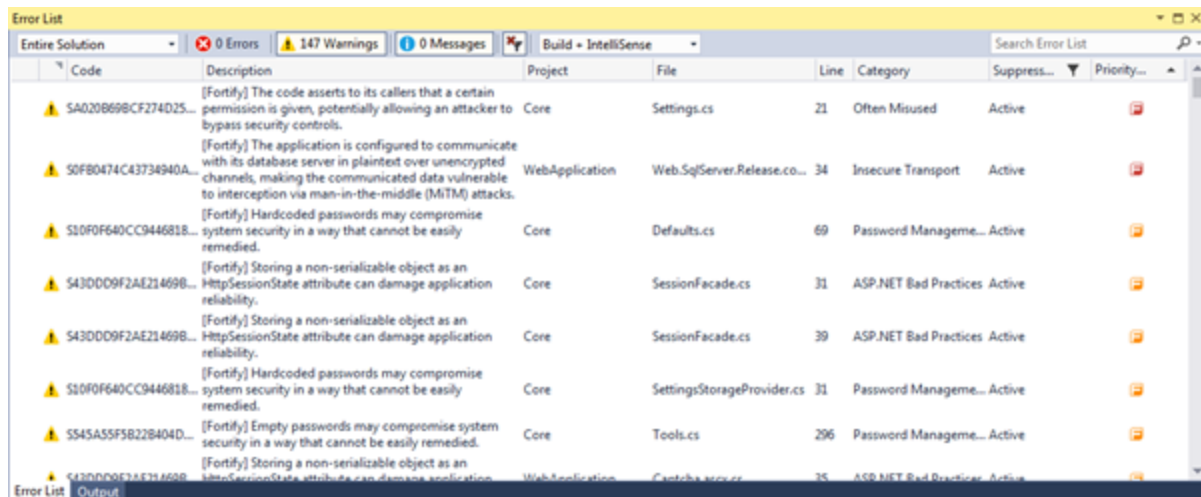
> **Tip:** To change how the issues are grouped, right-click the **Error List**, and then select **Grouping**.

The following table describes the Fortify information provided for each issue.

Column	Description
Description	A brief description of the issue. Fortify Security Assistant prepends each detected issue with `[Fortify]`.
Category	The Fortify category.
Suppression State	Indicates whether or not the issue has been suppressed (hidden). To change whether suppressed issues are visible or not, click the filter icon in the **Suppression State** column, and then select or clear the **Suppressed** check box.

Column	Description
Priority Order	A colored icon indicates the Fortify Priority Order used to categorize the severity of a vulnerability. • ▣ Critical • ▣ High • ▣ Medium • ▣ Low

Suppressing Categories of Issues

As you review the issues, you might want to completely suppress some exposed issues. It is useful to suppress issues if you are sure that the vulnerability category is not, and will never be, an issue of concern. You might also want to suppress warnings for specific issue categories that might not be high priority or of immediate concern.

You can suppress issue categories for the entire solution. The issue category is not reported again for the solution unless you unsuppress it (see "Unsuppressing Categories of Issues" below).

To suppress an issue category:

1. Open the **Error List** window if it is not currently open.

2. In the **Error List** window, right-click an issue, and then select **Suppress Category**.

Categories of issues that you suppress are stored in a `.FortifyIgnore` file with your Visual Studio solution file. You can share this file with other members of your organization. For more information about this Fortify issue suppression file, see "Using the Fortify Issue Suppression File" on the next page.

Suppressed issues are no longer highlighted in the code as a Fortify issue. The visibility of suppressed issues in the **Error List** window depends on the filter setting for the **Suppression State** column).

Unsuppressing Categories of Issues

To unsuppress an issue category:

1. Open the **Error List** window if it is not currently open.

2. To make sure that suppressed issues are visible, click the filter icon in the **Suppression State** column, and then select the **Suppressed** check box.

3. Right-click an issue, and then select **Unsuppress Category**.

The issue category is no longer suppressed in the solution.

To unsuppress all issues for the solution, remove (or rename) the `.FortifyIgnore` file that is located with the solution file.

Using the Fortify Issue Suppression File

You can use the Fortify issue suppression file to suppress categories of issues and to exclude files or directories from having any issues reported. You can share this file with other members of your organization.

Fortify Security Assistant creates the Fortify issues suppression file (`.FortifyIgnore`) in the same directory as your project solution when you first suppress an issue category. You can edit this file using a text editor. After you make changes to the issue suppression file, re-analyze your solution to apply the suppressions.

Each line in this file can contain either:

- Suppression of a Fortify category

  Specify the full Fortify category to suppress issues of that category for all files in the project. Fortify Security Assistant adds an line to the `.FortifyIgnore` file each time you suppress a category in the **Error List** window.

  For example:

  ```
  ASP.NET Misconfiguration: Debug Information
  Poor Error Handling: Overly Broad Catch
  Cookie Security: HTTPOnly not Set on Application Cookie
  ```

- Suppression of all issues in one or more files

  For example, you might want to use this to suppress all issues in files that contain generated code.

  The syntax for this type of suppression follows these rules:

  - The first character must be a slash (/) or backslash (\).

  - Use a single asterisk (*) to represent zero or more file name characters.

  - Use two asterisks (**) to represent zero or more directories or all directory contents when specified at the end of the line.

  - Paths must be relative to the `.FortifyIgnore` file location. You can use either the slash or backslash as the directory separator.

  For example, the following line suppresses all issues for any file with the `.cs` extension in the `Generated` directory:

  ```
  /**/Generated/*.cs
  ```

  The following example suppresses all issues in one specific file:

  ```
  /my/full/path/file.config
  ```

The following example suppresses all issues in all files with the `.aspx` extension in the root solution directory:

```
/*.aspx
```

The following example suppresses all issues for all files in the `test` directory:

```
/test/**
```

Send Documentation Feedback

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

Feedback on User Guide (Fortify Security Assistant Extension for Visual Studio 18.10)

Just add your feedback to the email and click send.

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

We appreciate your feedback!