

# Fortify Security Assistant Plugin for IntelliJ and Android Studio

Software Version: 24.1

## User Guide

Document Release Date: February 2024

Software Release Date: February 2024

## Legal Notices

Open Text Corporation

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

## Copyright Notice

Copyright 2022-2024 Open Text.

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

## Trademark Notices

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

## Documentation Updates

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

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

This document was produced on February 29, 2024. 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 .....	4
Contacting Fortify Customer Support .....	4
For More Information .....	4
About the Documentation Set .....	4
Fortify Product Feature Videos .....	4
Change Log .....	5
Getting Started .....	6
Fortify Security Assistant Requirements .....	6
Installing Fortify Security Assistant .....	7
Configuring Fortify Security Assistant .....	8
Finding Security Issues as you Write Code .....	10
Viewing Vulnerability Details .....	11
Suppressing Issues .....	12
Scanning a Project for Security Issues .....	12
Disabling Vulnerability Categories .....	13
Enabling Vulnerability Categories .....	14
Working with the Fortify Security Assistant Window .....	15
Troubleshooting .....	16
Send Documentation Feedback .....	17

# Preface

## Contacting 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/cyberres/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 OpenText Product Documentation website:

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

To be notified of documentation updates between releases, subscribe to Fortify Product Announcements on the OpenText Community:

<https://community.microfocus.com/cyberres/fortify/w/fortify-product-announcements>

## Fortify Product Feature Videos

You can find videos that highlight Fortify products and features on the Fortify Unplugged YouTube channel:

<https://www.youtube.com/c/FortifyUnplugged>

# 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.

<b>Software Release / Document Version</b>	<b>Changes</b>
24.1	Updated: <ul style="list-style-type: none"><li>• Added information about how to apply plugin provided code fixes to automatically remediate vulnerability issues (see <a href="#">"Finding Security Issues as you Write Code" on page 10</a> and <a href="#">"Working with the Fortify Security Assistant Window" on page 15</a>)</li><li>• Added content for ability to use the IDE's storage for trusted certificates (see <a href="#">"Configuring Fortify Security Assistant" on page 8</a>)</li></ul>
23.1	Updated version and release date
22.2	Updated: <ul style="list-style-type: none"><li>• Added a requirement for downloading security content from OpenText™ Fortify Software Security Center (<a href="#">"Fortify Security Assistant Requirements" on the next page</a>)</li></ul>

# Getting Started

The Fortify Security Assistant Plugin for IntelliJ (Fortify Security Assistant) works with a portion of the Fortify security content to provide alerts to potential security issues as you write your Java code. Fortify Security Assistant provides quick-fix actions for some vulnerabilities, 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 configurations in property and XML files

Fortify Security Assistant notifies you of any detected issues as you write your code. You can also examine an entire project and then review the detected security issues.

**Note:** The instructions in this guide 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.

## Fortify Security Assistant Requirements

Fortify Security Assistant requires:

- A valid Fortify license file  
For information about how to obtain a Fortify license, contact Customer Support.
- Up-to-date Fortify Secure Coding Rulepacks (Fortify security content)  
Fortify Security Assistant uses a knowledge base of rules to enforce secure coding standards applicable to the codebase for static analysis. The Fortify Secure Coding Rulepacks describe general secure coding idioms for popular languages and public APIs.

From Fortify Security Assistant, you can:

- Download the Fortify security content directly from the Fortify Rulepack update server or from a Fortify Software Security Center server.

**Important!** To download security content from a server that is configured to use HTTPS, you must first import a self- or locally-signed certificate into the Java Runtime Environment (JRE) certificate store. See the IntelliJ IDEA or Android Studio documentation for more information. The following are examples of the certificate storage location:

IntelliJ IDEA: `<IDE_install_dir>/jbr/lib/security/cacerts`

Android Studio: `<IDE_install_dir>/jre/lib/security/cacerts`

You can also use the IDE's storage for trusted certificates (see ["Configuring Fortify Security Assistant" on the next page](#)).

- Import Fortify security content from your local system.  
You might choose this option if you do not have a network connection to a server.

### See Also

["Configuring Fortify Security Assistant" on the next page](#)

## Installing Fortify Security Assistant

You can install Fortify Security Assistant on Windows, Linux, and macOS. The Fortify Security Assistant plugin is available for download from the JetBrains Marketplace.

To install Fortify Security Assistant:

1. Start IntelliJ IDEA or Android Studio.
2. Open **Settings** or **Preferences**.
3. In the left pane, select **Plugins**.
4. Select the **Marketplace** tab, and then in the search box type Fortify Security Assistant.
5. Select the Fortify Security Assistant Plugin for IntelliJ and then click **Install**.
6. Click **OK**.

If this is the first time you installed Fortify Security Assistant, you must next specify the Fortify license file and load Fortify security content (see ["Configuring Fortify Security Assistant" on the next page](#)).

## Configuring Fortify Security Assistant

In order for Fortify Security Assistant to detect vulnerabilities in your code, you must have a valid Fortify license file and up-to-date Fortify security content. You can download Fortify security content from the Fortify Rulepack update server (<https://update.fortify.com>), or from a Fortify Software Security Center server.

If you do not have a network connection to the Fortify Rulepack update server or a Fortify Software Security Center server, Fortify Security Assistant can load Fortify security content from a local folder.

To configure Fortify Security Assistant:

1. Open **Settings** or **Preferences**.
2. In the search box, type `fortify`.
3. Select **Fortify Security Assistant** in the left pane.

The screenshot shows the 'Fortify Security Assistant' configuration window. At the top, there is a breadcrumb 'Other Settings > Fortify Security Assistant' and a 'Reset' button with left and right navigation arrows. The window is divided into several sections:

- License**: A text field for 'License file:' with a folder icon (Browse) to its right.
- Security Content**:
  - Use local Rulepack
    - Folder: [text field] [folder icon]
    - Load Security Content [button]
  - Use security content server
    - URL: [text field with 'https://update.fortify.com'] [button with 'Default']
    - Software Security Center
    - Security content date: Not Updated [button with 'Check for Updates']
- Use IDE certificate management system
- Use proxy
  - Server: [text field]
  - Port: [text field with '80' and a spinner]
  - User name: [text field]
  - Password: [text field]

4. To specify the license file, click **Browse** to the right of the **License file** box and navigate to the license file (`fortify.license`) on your system.



5. To load or update Fortify security content stored locally:
  - a. Select **Use local Rulepack**.
  - b. Click **Browse** next to the **Folder** box and navigate to a folder on your system that contains the Rulepacks.

The selected folder must contain Rulepacks as ZIP, XML, or BIN files.
  - c. Click **Load Security Content**.
6. To download Fortify security content from a Rulepack update server or from Fortify Software Security Center:
  - a. Select **Use security content server**.
  - b. To download security content from the Fortify Rulepack update server, in the **URL** box, type a Rulepack server URL.

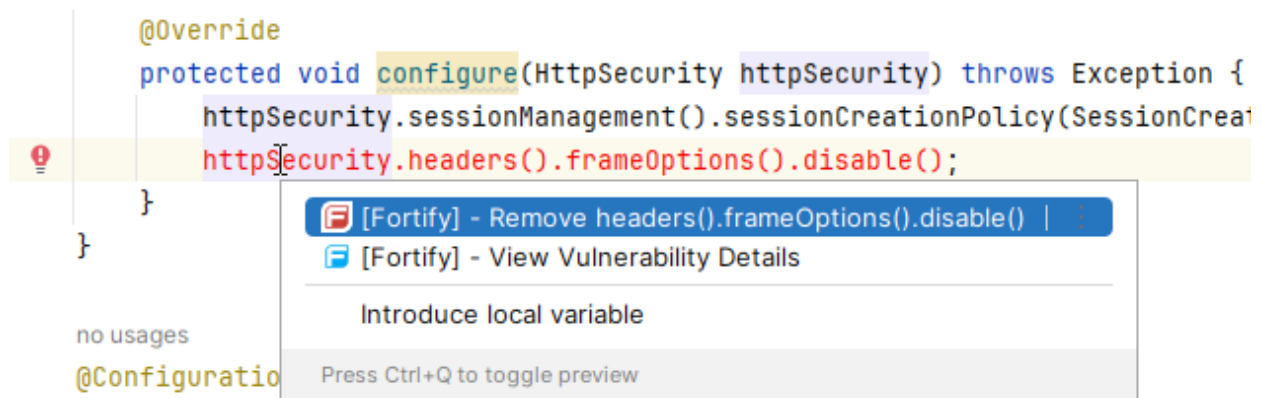
The default is the Fortify Rulepack update server URL (<https://update.fortify.com>).

**Note:** Click **Default** to set the URL to the default Fortify Rulepack update server.
  - c. To download security content from Fortify Software Security Center:
    - i. In the **URL** box, type a Fortify Software Security Center URL.
    - ii. Select the **Software Security Center** check box.
  - d. To connect to the security content server through a proxy server, select **Use proxy**, and then provide the following:
    - The proxy server host name (for example, my.proxy.com)
    - The proxy port number
    - (Optional) Authentication credentials for the proxy server
  - e. 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 Customer Support for assistance.
7. To use the IDE's storage for trusted certificates, select **Use IDE certificate management system**.
8. Click **OK**.

# Finding Security Issues as you Write Code

As you review the code inspections in the code editor, Fortify Security Assistant provides a detailed description of the Fortify-detected issues and can include an automatic remediation fix in the interactive preview. Critical issues are shown in red in the code editor. Fortify Security Assistant also provides notifications of security issues in the **Fortify Security Assistant** window and the IDE **Problems** tool window.

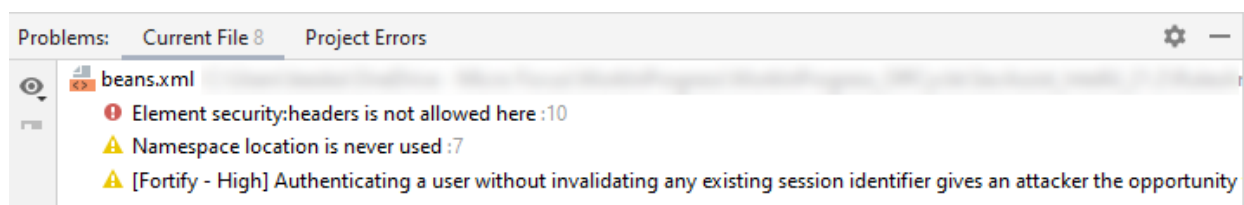


In the code editor, place the cursor over the line of code that is marked as an issue, and do one of the following:

- Click to apply the suggested fix if available
- Click **View Vulnerability Details**

The Fortify Security Assistant **Vulnerability Details** window opens and provides a detailed description of the issue, examples, and recommendations of how to fix the issue.

Detected issues displayed in the **Problems** window are prefixed with `[Fortify - <priority>]` as shown in the following example:



## See Also

["Viewing Vulnerability Details" on the next page](#)




["Scanning a Project for Security Issues" on page 12](#)

## Viewing Vulnerability Details

To see a detailed description of an issue, from the code editor or the **Fortify Security Assistant** window, right-click the issue, and then select **View Vulnerability Details**.

The **Vulnerability Details** window provides a detailed description of the issue, examples, and recommendations of how to fix the issue.

### Vulnerability Details

**Category**

(XXE) XML External Entity Injection

**Abstract**

Using XML parsers configured to not prevent nor limit external entities resolution can expose the parser to an XML External Entities attack.

**Explanation**

XML External Entities attacks benefit from an XML feature to build documents dynamically at the time of processing. An XML entity allows inclusion of data dynamically from a given resource. External entities allow an XML document to include data from an external URI. Unless configured to do otherwise, external entities force the XML parser to access the resource specified by the URI, e.g., a file on the local machine or on a remote system. This behavior exposes the application to XML External Entity (XXE) attacks, which can be used to perform denial of service of the local system, gain unauthorized access to files on the local machine, scan remote machines, and perform denial of service of remote systems. The following XML document shows an example of an XXE attack.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
  <!DOCTYPE foo [
    <!ELEMENT foo ANY >
    <!ENTITY xxe SYSTEM "file:///dev/random" >]><foo>&xxe;</foo>
```

This example could crash the server (on a UNIX system), if the XML parser attempts to substitute the entity with the contents of the /dev/random file.

XML parsers can be configured to enable and disable certain features for performance and

## Suppressing Issues

You might want to suppress warnings for specific issues that might not be high priority or of immediate concern.

To suppress issues, use the native IntelliJ IDEA or Android Studio suppress inspections feature in the code editor. You can suppress issues from the code editor and the **Problems** window.

For more information about re-enabling suppressed inspections, see the documentation for your IDE.

The visibility of suppressed issues in the **Fortify Security Assistant** window depends on the setting for the **Suppressed** column). For instructions on how to change the visibility of suppressed issues, see ["Working with the Fortify Security Assistant Window" on page 15](#).

### See Also

["Disabling Vulnerability Categories" on the next page](#)

## Scanning a Project for Security Issues

You can analyze the whole project (or a specific set of files) and identify security issues. You cannot make any code changes during the analysis.

To scan a project for issues:

- Run the IDE code inspection.

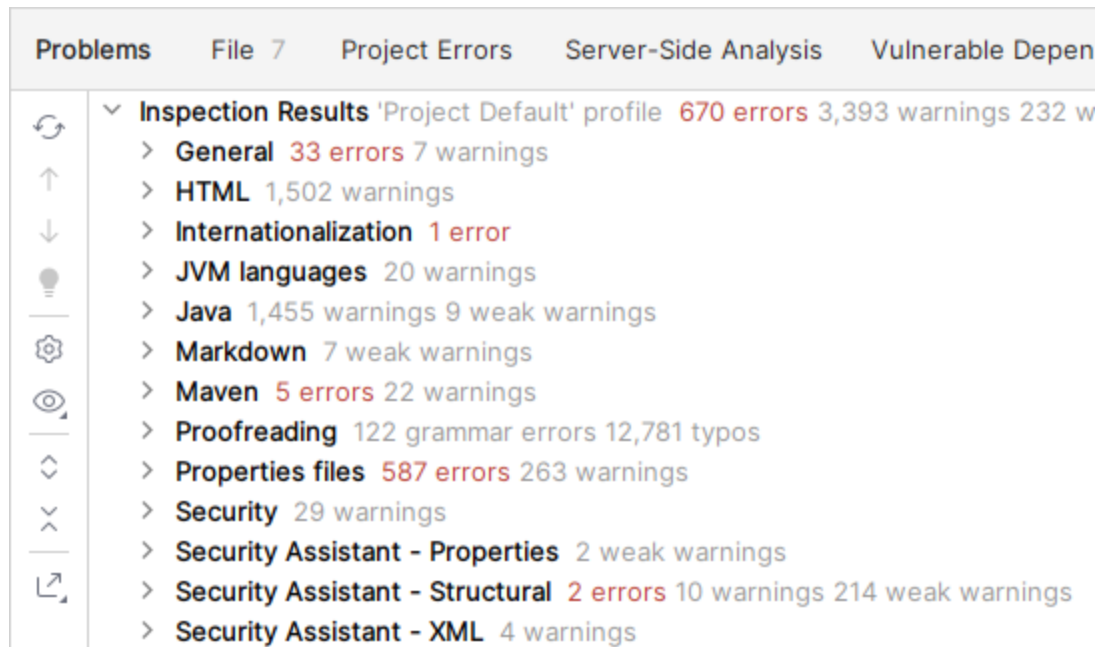
If you see the following message in the Event Log:

```
Please wait for the security content (Rulepack) to be loaded. Security content is required to detect vulnerabilities.
```

Then wait until the Fortify security content is loaded. Run the code inspection again after you see the following message:

```
Fortify Security Assistant is ready to work
```

Fortify Security Assistant displays any detected issues in the IntelliJ IDEA or Android Studio **Problems** window. The issues are grouped by analyzer as shown in the following example.



The detected security issues are also displayed in the **Fortify Security Assistant** window. For information about reviewing the security issues in the **Fortify Security Assistant** window, see ["Working with the Fortify Security Assistant Window" on page 15](#).

## Disabling Vulnerability Categories

As you review Fortify detected issues, you might want to completely disable a category of reported issues. It is useful to disable vulnerability categories if you are sure that the vulnerability category is not, and will never be, an issue of concern.

All issues in the disabled vulnerability categories are not reported again unless you re-enable them (see ["Enabling Vulnerability Categories" on the next page](#)).

To disable a vulnerability category, use the native IntelliJ IDEA or Android Studio disable inspection feature (**File > Settings > Editor > Inspections**). There are three groupings of Fortify Security Assistant vulnerability categories:

- Security Assistant - Properties
- Security Assistant - Structural
- Security Assistant - XML

**Note:** You can also disable a Fortify vulnerability category for a scanned project from the **Problems** window.

After you clear a check box for a vulnerability category, issues that fall into that vulnerability category are no longer highlighted in the code as a Fortify Security Assistant detected issue.

## Enabling Vulnerability Categories

To re-enable a Fortify vulnerability category that you have disabled, use the native IntelliJ IDEA or Android Studio re-enable inspection feature (**File > Settings > Editor > Inspections**). Locate the Fortify Security Assistant vulnerability category you want to re-enable and select the check box.

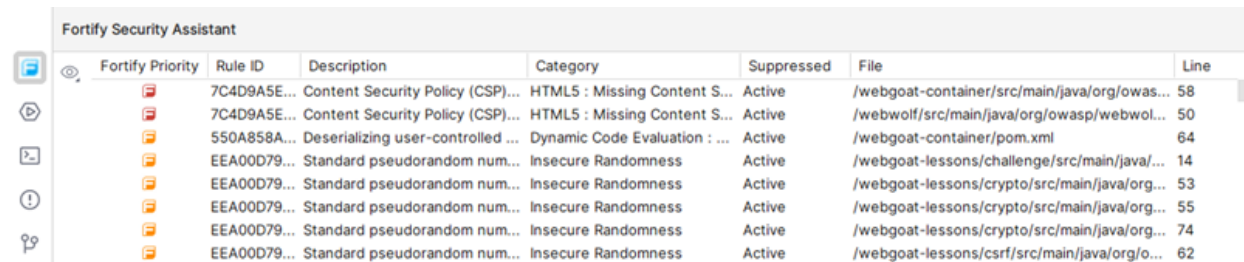
**Note:** You can also re-enable a vulnerability category for a scanned project from the **Problems** window. To refresh the issues displayed in the Fortify Security Assistant window after re-enabling a vulnerability category, rescan the project (see "[Scanning a Project for Security Issues](#)" on [page 12](#)).

### See Also

["Disabling Vulnerability Categories" on the previous page](#)

# Working with the Fortify Security Assistant Window

Fortify Security Assistant displays all the security issues detected as you write code and for open files in the **Fortify Security Assistant** window.



Fortify Priority	Rule ID	Description	Category	Suppressed	File	Line
	7C4D9A5E...	Content Security Policy (CSP)...	HTML5 : Missing Content S...	Active	/webgoat-container/src/main/java/org/owasp...	58
	7C4D9A5E...	Content Security Policy (CSP)...	HTML5 : Missing Content S...	Active	/webwolf/src/main/java/org/owasp/webwol...	50
	550A858A...	Deserializing user-controlled ...	Dynamic Code Evaluation : ...	Active	/webgoat-container/pom.xml	64
	EEA00D79...	Standard pseudorandom num...	Insecure Randomness	Active	/webgoat-lessons/challenge/src/main/java/...	14
	EEA00D79...	Standard pseudorandom num...	Insecure Randomness	Active	/webgoat-lessons/crypto/src/main/java/org...	53
	EEA00D79...	Standard pseudorandom num...	Insecure Randomness	Active	/webgoat-lessons/crypto/src/main/java/org...	55
	EEA00D79...	Standard pseudorandom num...	Insecure Randomness	Active	/webgoat-lessons/crypto/src/main/java/org...	74
	EEA00D79...	Standard pseudorandom num...	Insecure Randomness	Active	/webgoat-lessons/csrf/src/main/java/org/o...	62

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

Column	Description
Fortify Priority	Colored icon indicates the Fortify Priority Order used to categorize the severity of a vulnerability <ul style="list-style-type: none"><li> Critical</li><li> High</li><li> Medium</li><li> Low</li></ul>
Rule ID	Unique identifier of the rule that triggered the vulnerability detection
Description	Brief description of the issue
Category	Fortify vulnerability category
Suppressed	Indicates whether the issue has been suppressed <p><b>Note:</b> By default, suppressed issues are not visible in this window. To see suppressed issues in this list, select <b>View Options</b>, and then select <b>Show Suppressed</b>.</p>

Column	Description
File	Name of the file where the issue occurs. To change whether to show the file path or only the file name, select <b>View Options</b> , and then select <b>Show Short File Name</b> .
Line	Line number where the issue occurs in the file.

As you review the detected issues, you can do the following:

- Read more information about the vulnerability by right-clicking an issue, and then selecting **View Vulnerability Details**.

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

- Open the file and locate the line of code where the issue was found by clicking the issue.
- Show only issues where Fortify Security Assistant has a fix by selecting **View Options**, and then selecting **Show only Issues with a Fix**.
- Show issues for the current file only by selecting **View Options**, and then selecting **Show only Current File**.
- Group the issues by file name, Fortify Priority, Fortify Rule ID, or Fortify category by clicking **View Options** and then selecting the grouping you want.
- Change whether suppressed issues are visible by selecting **View Options**, and then selecting **Show Suppressed**.
- Copy the rule ID for an issue by right-clicking the issue, and then selecting **Copy Rule ID**.

### See Also

["Viewing Vulnerability Details" on page 11](#)

["Suppressing Issues" on page 12](#)

## Troubleshooting

For help diagnosing a problem, you can open the Fortify Security Assistant log file from the IDE. To open the log file, select **Help > Show Fortify Security Assistant Log**. If you contact Customer Support, provide them with this log file.



# Send Documentation Feedback

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

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

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

**Feedback on User Guide (Fortify Security Assistant Plugin for IntelliJ and Android Studio 24.1)**

Just add your feedback to the email and click send.

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

We appreciate your feedback!