OpenText™ Fortify Code Security Plugin for JetBrains IDE Tools

User Guide

Version : 26.3

Table of Contents

1. User Guide

Software Version: 26.3

Document Release Date: July 2026

Software Release Date: July 2026

1.1. 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
26.3	Initial version and release

1.2. Introduction

The Fortify Code Security Plugin for JetBrains IDE Tools provides an integrated application security workflow inside JetBrains IDE tools to support early identification and remediation of vulnerabilities. Use the Fortify Code Security Plugin for JetBrains IDE Tools to authenticate, select target applications, run scans, and remediate findings across Fortify on Demand and Application Security.

The plugin enables local SAST scans using Fortify SAST, submission of remote scans through ScanCentral SAST, and project uploads to Fortify on Demand for both SAST and Fortify Software Composition Analysis (Fortify SCA), all from within JetBrains IDE tools.

Security findings are displayed directly in the editor and linked to their corresponding source-code locations for efficient review. The plugin also integrates OpenText Fortify Remediation Aviator to provide AI-assisted remediation, including contextual explanations and one-click code fixes for supported vulnerabilities. By embedding these capabilities into the development workflow, the plugin reduces context switching and streamlines security remediation during coding.

With this plugin, you can:

- Generate dynamic command UI based on preferred platform (Fortify on Demand or Application Security Center).
- Orchestrate platform-aware workflow for Fortify on Demand and Application Security Center.
- Authenticate to Fortify on Demand or Application Security Center from the sidebar.
- Select application version/release to scan and remediate.
- Run scans locally with SAST, translate remotely with ScanCentral SAST, or retrieve existing issues.
- Review and audit vulnerabilities in the remediation panel.
- Apply AI-assisted remediations using Fortify Remediation Aviator auto-remediation.

Advanced features

- Save configurations for repeated tasks in Favorites.
- Sidebar actions for authentication, application selection, start scan, remediation, and auto-remediation (for Application Security Center workflows only).
- Use JetBrains AI Assistant or GitHub Copilot to perform tasks across both Fortify on Demand and Application Security Center. Use JetBrains AI Chat or

GitHub Copilot Chat to query vulnerabilities via Skills and MCP servers.

- Interact with the plugin using fcli commands via **FCli: Discover Resources & Commands**.

1.2.1. Software requirements

This topic describes the OpenText Application Security Software that the plugin works with and the requirements for each task.

Before you use the plugin, make sure the following requirements are met.

Software	Version	Requirements
Fortify on Demand	N/A	To upload your project to Fortify on Demand for assessment, make sure that you have the following: • ScanCentral SAST standalone client installed and configured explicitly in the plugin settings. • Fortify on Demand credentials and personal access tokens.
Fortify SAST (Fortify Static Code Analyzer)	24.2.0 or later	To scan your project locally with Fortify SAST, you must have the full path to the sourceanalyzer executable. Make sure that your system meets the requirements for the Fortify SAST version you are using as described in the *Fortify SAST User Guide* in Static Application Security Testing Documentation.

Software	Version	Requirements
Application Security (Software Security Center)	24.2.0 or later	To upload analysis results to Application Security after an analysis with ScanCentral SAST, make sure you have the following: • An application version that exists in Application Security • An authentication token of type `ToolsConnectToken` or `CIToken`
ScanCentral SAST	24.2.0 or later	(Optional) To scan your project remotely with ScanCentral SAST, make sure that you have a ScanCentral SAST client authentication token. For languages that are supported for analysis and system requirements for the ScanCentral SAST version you are using, see the *Fortify Software System Requirements* document in Application Security Center Documentation.

- Install the preferred JetBrains IDE tool from JetBrains with the following version requirements.

  - Intellij IDEA 2026.2 or later
  - PyCharm 2026.2or later
  - WebStorm 2026.2 or later
- Install Fortify Code Security Plugin for JetBrains IDE Tools from the JetBrains Marketplace.
- Install fcli version 3.21.0 or later (the plugin automatically installs or updates fcli if **Automatically install/update fcli** is selected in the plugin settings) and ensure fcli executable path is configured explicitly in the plugin settings.
- Ensure you have access to Fortify on Demand or Application Security Center and the required credentials or tokens.
- For local SAST scans, install OpenText SAST locally.
- For remote scans, install ScanCentral client locally or use the **Install or update ScanCentral client** settings to install or update the ScanCentral client. For more information, see Configuring the Fortify Code Security Plugin.
- To audit issues in the analysis results, your user account must have audit permissions.
- To add comments to issues or assign custom tags that require comments, your user account must have the permission to comment on issues.
- For JetBrains AI Chat assisted workflows, ensure JetBrains AI Assistant plugin is installed. For more information, see Using JetBrains AI Assistant with the Fortify Code Security Plugin.
- For Github Copilot Chat assisted workflows, ensure GitHub Copilot plugin is installed. For more information, see Using GitHub Copilot with the Fortify Code Security Plugin.

1.2.2. Installing the Fortify Code Security Plugin for JetBrains IDE Tools

You can install the plugin on Windows, Linux, or macOS.

You can install the plugin on the following JetBrains IDE tools:

- IntelliJ IDEA
- PyCharm
- WebStorm

To install the plugin, search `Fortify Code Security` in the JetBrains Marketplace.

For more information and instructions about how to install an plugin, see the *JetBrains Documentation*.

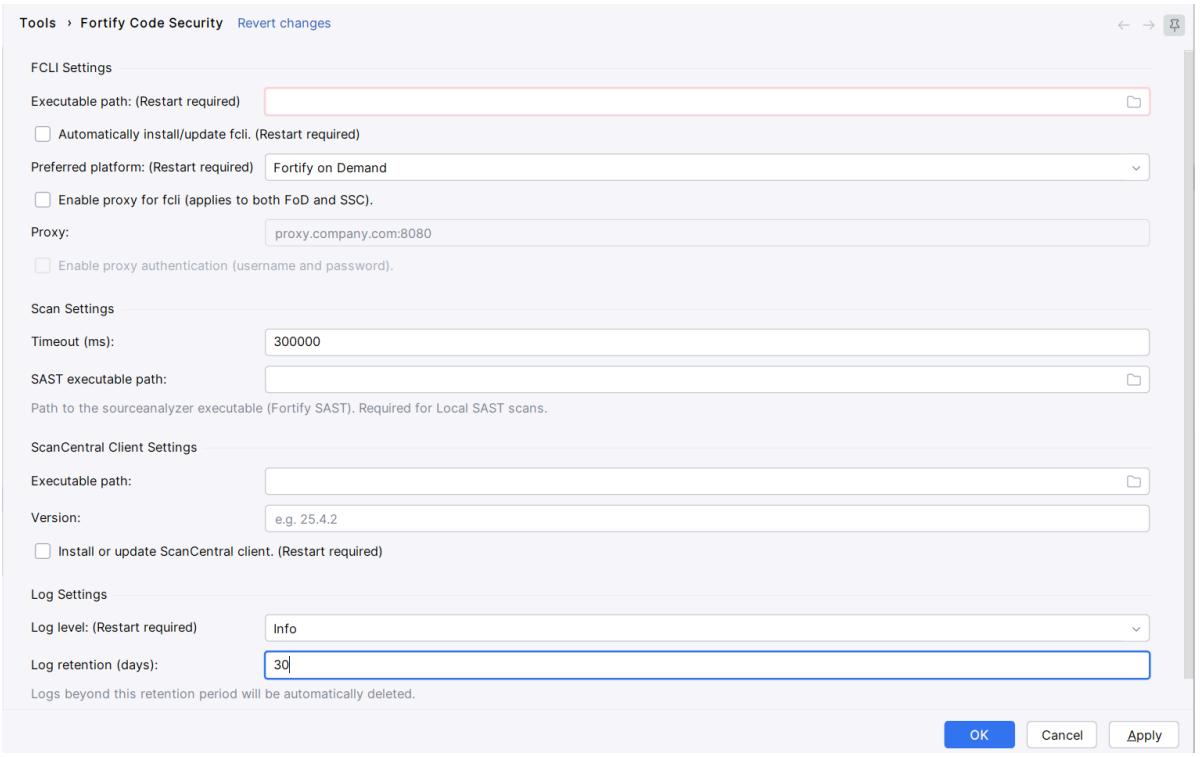
After you install the Fortify Code Security Plugin for JetBrains IDE Tools, the IDE Tool Window now includes the Fortify Code Security menu.

1.2.3. Configuring the Fortify Code Security Plugin

To configure the Fortify Code Security Plugin for JetBrains IDE Tools plugin settings:

1. Click **Fortify Code Security** in the tool window and click **SETTINGS** in the sidebar.

   The Settings window displays.



2. Configure the following properties for Fortify Code Security Plugin:

Property	Description
FCLI Settings	
Executable path	Required. Path to the fcli executable. Click **Browse...** to select the executable file. **Example** *<home directorv>/fcli-windows/fcli.exe* Restart IDE to apply the changes.
Automatically install/update fcli	Optional. Select this property to automatically install or update the fcli version. Restart IDE to apply the changes.
Preferred Platform	Required. Specifies the preferred platform. You can either select Application Security Center (SSC) or Core Application Security (FoD).
Enable proxy for fcli	(Optional) Select the check box if your environment requires a proxy server to connect to Application Security Center (SSC) or Core Application Security (FoD).
Proxy	(Required if **Enable proxy for fcli** is selected). Type the host name and port number of the proxy server. Use the following format: `host:port` Example: `proxy.company.com:8080`

Property	Description
Enable proxy authentication	(Required if **Enable proxy for fcli** is selected). Select the check box if the proxy server requires authentication. The Configure Proxy Credentials box is displayed. Type the **Proxy username** and **Proxy password** for the proxy server and click **Save**.
Scan Settings	
Timeout (ms)	Optional. Specifies the timeout for any operations in milliseconds. Default: `300000` (5 minutes)
SAST executable path	Required for local SAST scans. Specifies the path to the locally installed Fortify SAST executable `sourceanalyzer.exe` (on Windows) or `sourceanalyzer` (on non-Windows).
ScanCentral Client Settings	

Property	Description
Executable path	Specifies the file path to ScanCentral SAST client executable. Go to the ScanCentral SAST installation directory and do one of the following: If you are using a standalone client installed with OpenText™ Application Security Tools, navigate to `<tools_install_dir>/bin/` and select `scancentral.bat` (on Windows) or `scancentral` (on non-Windows). If the standalone client is installed in a different location, navigate to the installation directory and select `scancentral.bat` (on Windows) or `scancentral` (on non-Windows). Restart IDE to apply the changes. **Note** You cannot configure both **ScanCentral Client: Executable Path** and **ScanCentral Client: Version** at the same time. Select one option to specify or install the ScanCentral client (`scancentral.bat` or `scancentral`).

Property	Description
Version	Optional. Specifies a version of ScanCentral client to install. Use the following version format: `Major.Minor.Patch` Example: 26.3.0 Restart IDE to apply the changes. **Note** You cannot configure both **ScanCentral Client: Executable Path** and **ScanCentral Client: Version** at the same time. Select one option to specify or install the ScanCentral client (`scancentral.bat` or `scancentral`).
Install or update ScanCentral client	Optional. Enables automatic ScanCentral client install or update through fcli. Restart IDE to apply the changes.
Log Settings	

Property	Description
Log level	Specifies the level of detail written to the plugin log file. Select one of the following options: **Info**: Logs standard operational messages, such as scan start and completion, authentication status, warnings, and errors encountered during normal use. **Debug**: Logs detailed diagnostic information in addition to all messages recorded at the **Normal** level. This includes `fcli` and ScanCentral command invocations, request and response payloads, and internal processing details. **Recommendation** Use this level when troubleshooting issues or when Customer Support requests log files for analysis. Because Debug logging can generate significantly larger log files and may capture sensitive information, switch back to Normal after troubleshooting is complete. **Default**: **Normal.** Restart IDE to apply the changes.
Log retention (days)	Specifies how long plugin log files are retained. Log files are generated weekly, and any log files older than the configured retention period are automatically deleted. **Default**: 30 days

3. Click **Apply** to apply the settings.
4. Click **OK.**
5. When prompted, restart IDE to apply the changes.

1.2.4. Related Documents

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

All Products

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

Document / File Name	Description
About Fortify Software Documentation appsec-docs-n-*<version>*.pdf	This paper provides information about how to access OpenText Application Security Software product documentation. **Note** This document is included only with the product download.
Fortify Software System Requirements appsec-sr-*<version>*.pdf	This document provides the details about the environments and products supported for this version of OpenText™ Application Security Software.
OpenText™ Application Security *Software Release Notes* appsec-rn-*<version>*.pdf	This document provides an overview of the changes made to OpenText™ Application Security Software for this release and important information not included elsewhere in the product documentation.
What's New in OpenText™ Application Security *Software <version>* appsec-wn-*<version>*.pdf	This document describes the new features in OpenText™ Application Security Software products.

OpenText™ ScanCentral SAST

The following document provides information about OpenText™ ScanCentral SAST. Unless otherwise noted, this document is available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-software-security-center.

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

OpenText™ Application Security

The following document provides information about OpenText™ Application Security. Unless otherwise noted, this document is available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-software-security-center.

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

Fortify SAST

The following documents provide information about Fortify SAST. Unless otherwise noted, these documents are available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-static-code-analyzer-and-tools.

Document / File Name	Description
Fortify SAST User Guide sast-ugd-*<version>*.pdf	This document describes how to install and use Fortify SAST to scan code on many of the major programming platforms. It is intended for people responsible for security audits and secure coding.
Fortify SAST Custom Rules Guide sast-cr-ugd-*<version>*.zip	This document provides the information that you need to create custom rules for Fortify SAST. This guide includes examples that apply rule-writing concepts to real-world security issues. **Note** This document is included only with the product download.
Fortify License and Infrastructure Manager Installation and Usage Guide lim-ugd-*<version>*.pdf	This document describes how to install, configure, and use the Fortify License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.

OpenText Application Security Tools

The following documents provide information about Fortify SAST applications and tools. Unless otherwise noted, these documents are available on the Product

Documentation website at https://www.microfocus.com/documentation/fortify-static-code-analyzer-and-tools.

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

1.3. Using Fortify Code Security Plugin with Fortify on Demand

You must have the standalone ScanCentral SAST client on the system where Fortify Code Security Plugin for JetBrains IDE Tools is installed to upload code to Fortify on Demand.

Requirements

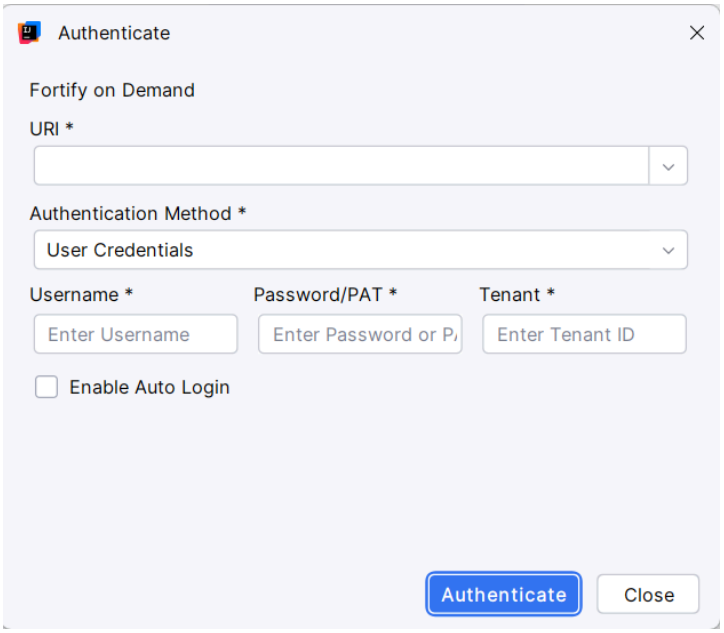
- fcli must be installed (the plugin automatically installs or updates fcli if **Fcli: Auto Update** is selected in the plugin settings) and configured with **Fcli: Executable Path** property in the plugin settings.
- The **Preferred Platform** in the plugin settings must be set to **Fortify on Demand (FoD)**.
- The Fortify on Demand tenant must have the required permissions to view applications, run scans, and update issue audit fields.

To upload the opened project to Fortify on Demand for assessment:

Authenticate your Fortify on Demand account

1. If the plugin is not open, click **Fortify Code Security** in the tool window.
2. Click **AUTHENTICATE** in the sidebar.

   The Authentication box is displayed in the VS Code Editor.



3. In the **URI**, you can either select one of the available URIs or type a valid URI.

4. Select an authentication method and provide the relevant credentials described in the following table.

Authentication method	Procedure
Username Credentials	1. In the **Username** box, type the account username. 2. In the **Password/PAT** box, type the account password or the personal access token. 3. In the **Tenant** box, type the tenant ID.
Client Credentials	1. In the **Client ID** box, type the API key. 2. In the **Client Secret** box, type the API secret.
Enable Auto Login	(Optional)Select the check box to securely store credentials and automatically restore expired sessions or silently re-authenticate when a session is missing or expired. No login prompts are displayed.

5. Click **AUTHENTICATE**.

   Upon successful authentication, **Fortify - Authenticated** status is displayed in the Notifications. Otherwise, the status displays **Not Authenticated**.

   To modify the URi, authentication method, or credentials, click **AUTHENTICATE** again.

Select Application and Release

1. Click **SELECT APPLICATION** in the sidebar.
2. In the **Select Application** box, select an application from the **Application Name** list.

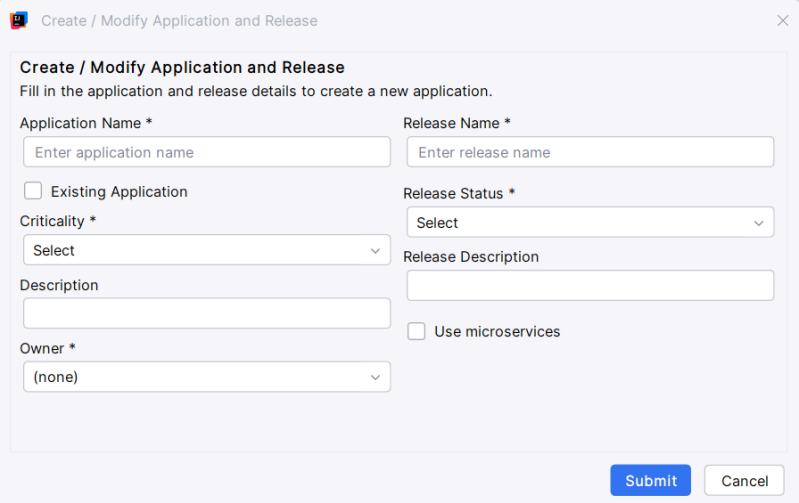
> **Note**
> Only 50 entries are displayed in the **Application Name** list.
> Use 3 or more characters to search for an application.
> When you search for an application, the extension searches all the entries and lists only the initial 50 entries matching the search text from the search results.
> To view additional entries or search results, click **Load next 50...** to load the next set of 50, and repeat as needed.

3. Select a release from the **Release** list.

> **Note**
> Only 50 entries are displayed in the **Release** list.
> Use any number of characters to search for a release.
> When you search for a release, the extension searches all the entries and lists only the initial 50 entries matching the search text from the search results.
> To view additional entries or search results, click **Load next 50...** to load the next set of 50, and repeat as needed.

4. Alternatively, to create a new Application or Release or modify an existing application or release:
    1. click **Create/Modify Application**.

       The **Create/Modify Application & Release** box displays.



    2. Define the application. Fields are required, unless otherwise noted.

Property	Description
Application Name	Type the name of your application or use the **Existing Application** check box to modify an existing application.
Existing Application	(Optional) To modify an existing application, click the check box. Select or search for an application from the **Application Name** list. Use 3 or more characters to search for an application. When you search for an application, the extension searches all the entries and lists only the initial 50 entries matching the search text from the search results. To view additional entries or search results, click **Load next 50...** to load the next set of 50, and repeat as needed. When you select an application, the application attribute values are synced from Fortify on Demand and populated in the respective fields.

Business Criticality	Select the application's level of importance: ▪ **High**: Security issues could have catastrophic consequences for the business. ▪ **Medium**: Security issues would have non-trivial consequences, but ones which do not pose a life-or-death threat to the business. ▪ **Low**: Security issues can be ignored or addressed gradually as time permits
Use microservices	(**Web / Thick-Client** applications only) Select the check box to scan the application as a microservice application. Type the name of a microservice in the **Microservice name** box and click **Add.** The microservice is added. You can add up to 10 microservices. Select a microservice and click **-** to delete the microservice. **Important** The designation of a microservice application is permanent and cannot be changed after the application has been created.
Application Description	(Optional) Type a description of the application that will help you manage multiple applications.

Owner	(Optional) Owner of the release who receives email notifications of scan status updates to the release

3. After you specify the application details, you can define the release. Fields are enabled after you specify the application details. Fields are required, unless otherwise noted.

Property	Description
Release Name	Type the name of your release.
Existing Release	If you have selected the **Existing Application** check box, you can use the **Existing Release** check box to modify an existing release. Select or search for a release from the **Release Name** list. Use any number of characters to search for a release. When you search for a release, the extension searches all the entries and lists only the initial 50 entries matching the search text from the search results. To view additional entries or search results, click **Load next 50 releases...** to load the next set of 50, and repeat as needed. When you select a release, the application release attribute values are synced from Fortify on Demand and populated in the respective fields.
Release Status	Select the Software Development Life Cycle stage of the release: **Development**, **QA**, **Production**. The **Retired** option is not available.
Select microservice (microservice applications only)	Select the microservice that will be linked to the release from the drop down list. A release must be linked to a microservice.
Release Description	(Optional) Type a description that helps describe the release.

4. Click **Submit**. The application name and release is displayed in the sidebar.

5. Click **Select Application.**

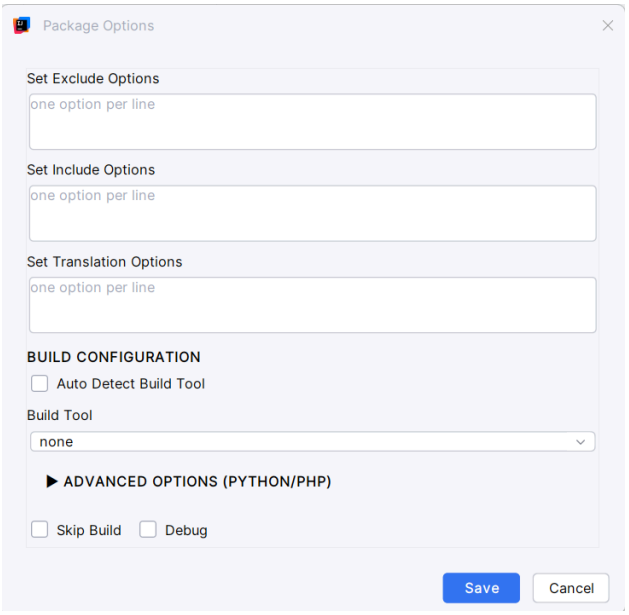
   The application name and release is displayed in the sidebar.

> **Note**
> You can add and modify custom attributes for application or releases that are marked Required for the Fortify on Demand tenant.

Scanning the Application

1. Click **START SCAN** in the sidebar.
2. In the **PACKAGE OPTIONS** area, click **View/Edit**.

   The Package Options box is displayed.



3. Provide the options described in the following table. All field are optional, unless otherwise noted.

Option	Description
Set Exclude Options	Specify the relative paths of files or directories to exclude from the package separated by a new line (one per line). You can use wildcard characters to specify the paths.
Set Include Options	Specify the relative paths of files or directories to include in the package separated by a new line (one per line). You can use wildcard characters to specify the paths. If you leave it empty, all the supported files are included.
Set Translation Options	Specify a list of Fortify SAST translation options separated by a new line (one per line).

Option	Description
Auto Detect Build Tool	Select this option to automatically detect the build tool. **Note** For .NET projects: ◦ On Windows, if you select the **Auto Detect build tool** option, the default build tool is MSBuild. ◦ On Linux, if you select the **Auto Detect build tool** option, the default build tool is DotNet. ◦ If you want to use DotNet as the build tool on a Windows, you must clear the **Auto Detect build tool** option and explicitly select **DotNet** from the **Build Tool** list. Selecting the **Auto Detect Build Tool** check box automatically hides the **Build Tool** list and **Advanced Options**.
Skip Build	Select whether to skip the build invocation that prepares the generated sources and libraries before the project information is packaged for submission to ScanCentral SAST.
Set Debug	Select this option to enable debug logging that can be helpful to troubleshoot issues.

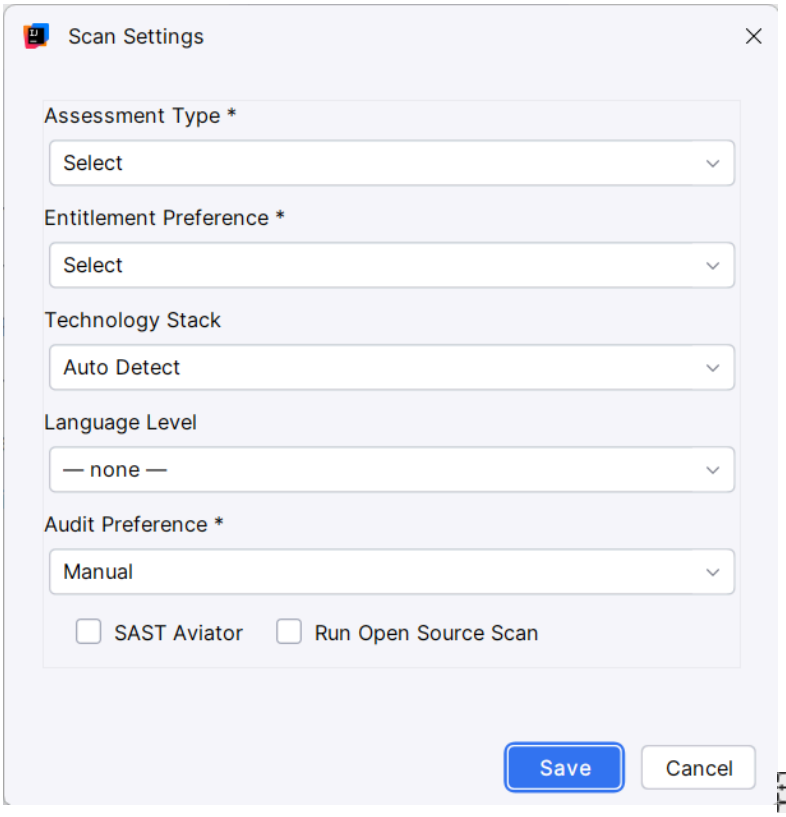
4. To select a build tool explicitly, clear the **Auto Detect Build Tool** check box and select a build tool in the **Build Tool** list and provide the settings based on the build tool.

Option	Description
Build File	(Optional) (For Gradle or Maven) Click **Browse..** icon and select the build file if it is different than the default of `build.gradle` or `pom.xml`. (For DotNet or MSBuild) Type the name of the build file. If you do not select a build file, ScanCentral SAST automatically detects the build file.
Build Command	(Optional) Type any custom build commands to prepare and build the project. If not specified, the default build command is used.
Advanced Options (Python/PHP) (applies only when you select None in the Build Tool list)	
PHP Version	(Optional) Type the PHP version used in the project.
Python Virtual Environment Location	(Optional) Click **Browse** and select the location (directory) of the Python virtual environment. Specify this together with the Python requirements file to have dependencies restored before the scan.

Option	Description
Python Requirements File	(Optional) Click **Browse** and select the Python project requirements file used to install and collect dependencies. Use only this Python field if you have no preference for the Python version used or there is only one Python version installed and on the PATH.
Python Version	(Optional) Select the Python version for Python projects.

5. Click **Save**.
6. In the **SCAN SETTINGS** area, you can select either a Static assessment or an open source software composition analysis in conjunction with a static assessment or as a separate open source only assessment.
    1. In the **Scan Settings** area, select **Static + Open Source.**
        1. If the status displays **Not Configured**, click **View/Edit**.

           The Scan Settings box displays.



2. Complete the fields as needed. All field are required, unless otherwise noted.

Field	Description
Assessment Type	Select the assessment type. Only assessment types allowed by the organization's security policy are displayed. By default, the plugin automatically populates the assessment type configured in Fortify on Demand.
Entitlement Preference	Select the entitlement that the assessment will use. The field displays entitlements that are valid for the selected assessment type, including those available for purchase. Note that microservice applications are restricted to subscriptions. If the release has an active subscription, only options that do not consume entitlements are displayed. By default, the plugin automatically populates the entitlement configured in Fortify on Demand.

Field	Description
Audit Preference	Select the audit preference. ▪ **Manual**: False positives identified by Fortify Audit Assistant with high confidence are automatically suppressed. A security expert then manually reviews the scan results. ▪ **Automated**: False positives identified by Fortify Audit Assistant with high confidence are automatically suppressed and results are published without manual review. **Note** If you select the Fortify Remediation Aviator check box, Automated audit is selected by default. If you change the **Audit Preference** to **Manual**, the **Fortify Remediation Aviator** check box is cleared automatically. The ability to select audit preference depends on the assessment type: ▪ A Static single scan allows Automated only.

Field	Description
	▪ A Static subscription allows one Manual audit per application (not per release or microservice). ▪ A Static+ single scan allows Manual only. ▪ A Static+ subscription allows Automated or Manual audit for each assessment. By default, the plugin automatically populates the audit preference configured in Fortify on Demand.
Technology Stack	Select the application's technology stack. The languages available for selection depends on the application type and whether the application is a microservice application. By default, the plugin automatically populates the technology stack configured in Fortify on Demand.
Language Level	If applicable, select the technology stack's language level from the list.

Field	Description
Fortify Remediation Aviator	(Optional) For scans using Automated audit, select the check box to have Fortify Remediation Aviator audit results and provide enhanced remediation assistance. By default, the plugin automatically selects or clears the check box as configured in Fortify on Demand.
Run Open Source Scan	(Optional) Select the check box to include open source software composition analysis. No code leaves the OpenText Fortify on Demand environment. By default, the plugin automatically selects or clears the check box as configured in Fortify on Demand.

3. Click **Save**.
4. Click **Start Scan** to upload a ScanCentral package to Fortify on Demand.

2. In the **Scan Settings** area, Select **Open Source Only**.
    1. If the status displays **File Not Selected**, click **Upload a File**.
    2. Browse and select the file. You can select **ZIP files** or **All Files** in the **File Type** list based on the file that you want to select.

       The status displays the zip file name or the current project.
    3. Click **Start Scan** to upload the package to Fortify on Demand.

7. If the project is successfully uploaded, the Fortify Code Security Plugin for JetBrains IDE Tools displays the completion status and the scan ID.

Remediating your code

After you select an application release, you can view the vulnerabilties and remediate.

Viewing and selecting vulnerabilities

To view and select vulnerabilities in the selected application release:

1. Click **REMEDIATE** in the sidebar.

   From the **Group By** list, select an attribute for sorting vulnerabilities in all visible folders into groups.

   The default grouping is **Category**.

2. Click a tab to view the associated vulnerabilities.

   Note
   The tabs shown depend on the issue severity of the application release.

   - The **Critical** tab contains issues that have a high impact and a high likelihood of exploitation. We recommend that you remediate critical issues immediately.
   - The **High** tab contains issues that have a high impact and a low likelihood of exploitation. We recommend 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. We recommend that you remediate medium issues as time permits.
   - The **Low** tab contains issues that have a low impact and a low likelihood of exploitation. We recommend that you remediate low issues as time permits (your organization can customize this category).
   - The **All** tab contains all issues.

   Within each tab, issues are grouped by vulnerability category. After each grouping name, enclosed in brackets, is the number of audited issues and the total number of issues in the group.

3. To view fixed and/or suppressed issues, click **Fixed** and/or **Suppressed** from the **Visibility** list.

4. Click to expand a grouping and view the issues it contains.

The Fortify Code Security Plugin for JetBrains IDE Tools retrieves the corresponding issues from Fortify on Demand.

5. Select an issue to view its details in the **ISSUE AUDIT** panel.
6. Click the **Refresh** icon to sync any changes to the issues in the application release in Fortify on Demand.

Grouping vulnerabilities

The following grouping options are available on the **REMEDIATE** section:

Group	Description
Assigned User	User defined
Auditor Status	Auditor issue remediation status.
Category	Issue category
CWE Top 25 2023	Common Weakness Enumeration Top 25 2023 classification
CWE Top 25 2024	Common Weakness Enumeration Top 25 2024 classification
CWE Top 25 2025	Common Weakness Enumeration Top 25 2025 classification
Developer Status	Developer issue remediation status
FISMA	FISMA classification (deprecated)
Fortify Aviator	Audited by Fortify Remediation Aviator
Attachments	Has attachments
Comments	Has Comments
NIST SP 800-53 Rev. 5	National Institute of Standards and Technology Special Publication 800-53
OWASP 2014 Mobile	OWASP mobile top 10 2014 classification
OWASP 2017	OWASP top 10 2017 classification
OWASP 2021	OWASP top 10 2021 classification
OWASP 2025	OWASP top 10 2025 classification

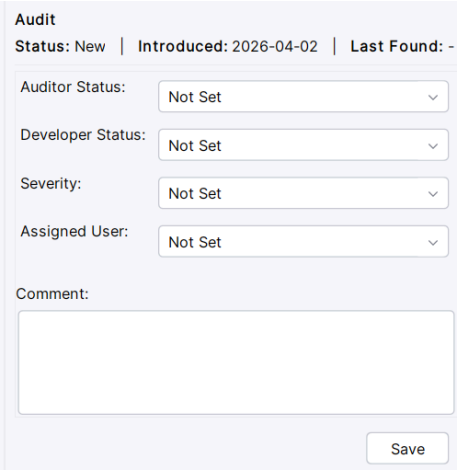
Group	Description
OWASP LLM Top 10 2025	OWASP LLM top 10 2025 classification
OWASP ASVS 4.0	OWASP ASVS 4.0 classification
OWASP ASVS 5.0	OWASP ASVS 5.0 classification
OWASP Mobile Top 10 2024	OWASP mobile top 10 2024 classification
Package	Package or namespace
PCI 4.0	PCI 4.0 classification
PCI 2.0	PCI 2.0 classification
PCI 3.0	PCI 3.0 classification
PCI 3.1	PCI 3.1 classification
PCI 3.2	PCI 3.2 classification
PCI SSF 1.2	PCI SSF 1.2 classification
Scan Type	Scan type to which issue belongs
Severity	Issue severity (filter only)
Sink	Dataflow sink function, applicable for static scan issues
Source	Dataflow source function, applicable for static scan issues
Status	Issue status
<Custom attribute>	User defined custom attributes

Viewing issue information

After you select an issue in the **ISSUE AUDIT** panel, the Fortify Code Security Plugin for JetBrains IDE Tools displays the issue-specific content in the **Fortify Issues** panel on the **Audit**, **Analysis Trace**, **Vulnerablity**, **Recommendations**, and **History** tab

Auditing issues

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



If you have the Edit Issues permission, you can assign a user, set the developer status, and add comments for issues in the Audit Summary view. If you have the Audit Issues permission, you can also edit the issue's auditor status and severity.
To audit an issue:

1. Make sure that the **Audit** panel is open.
2. From the issues list in the **REMEDIATE** section, select an issue. You can select multiple issues to make the same edits to multiple issues.
3. To change the auditor status, select the status from the **Auditor Status** list.
4. To change the issue's development status, select the status from the **Developer Status** list
5. To change the issue severity, select an issue severity from the **Severity** list.
6. Select the user to assign to the issue from **Assigned User** list.
7. To add a comment for the issue, type your comment in the box at the bottom of the **Comment** area..
8. Click **Save**.

   The changes and comments are displayed in the **History** tab.

The Fortify Code Security Plugin for JetBrains IDE Tools saves your changes for the selected application release.

Note

Any changes you make on the **Audit** tab are automatically uploaded to the application release in Fortify on Demand.

Analysis Trace

The **Analysis Trace** tab displays the relevant trace output. This is a set of program points that show how the analyzer found the issue. VS Code places the focus on the line of code that contains the selected security-related issue.

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 box shows the direction of the dataflow in this section of the source code.

Analysis Trace Icons

The analysis trace icons described in the following table show how dataflow moves in the section of the source code or execution order.

Icon	Description	Icon	Description
	Data is assigned to a field or variable		Tainted data is returned from a function
	Information is read from a source external to the code such as an HTML form or a URL		A pointer is created
	Data is assigned to a globally scoped field or variable		A pointer is dereferenced
	A comparison is made		The scope of a variable ends
	The function call receives tainted data		The execution jumps
	The function call returns tainted data		A branch is taken in the code execution

Icon	Description	Icon	Description
	Passthrough, tainted data passes from one place to another This is typically shown as functionA(x : y) to indicate that data is transferred from x to y. The x and y values are one of the following: • An argument index • `return` —The return value of a function • `this` —The instance of the current object • A specific object field or key		A branch is not taken in the code execution
	An alias is created for a memory location		Generic

Icon	Description	Icon	Description
	Data is read from a variable		A runtime source, sink, or validation step
	Data is read from a global variable		Taint change

Vulnerability

The **Vulnerability** tab displays the following technical details about the issue:

- Issue summary
- Explanation of the execution and implications of the issue
- Instance ID and primary rule ID
- Standards and best practices information from Fortify Software Security Research
- References
- Link to Secure Code Warrior Training Portal

Recommendations

The **Recommendations** tab displays remediation information and references for further research. The following table describes the sections on this tab.

Section	Description
Recommendations/Custom Recommendations	Describes possible solutions for the selected issue. It can also include examples and recommendations defined by your organization.
Tips/Custom Tips	Provides useful information specific to the selected issue, and any custom tips defined by your organization.
Secure Code Warrior	If available, this section contains links to interactive training for the issue category, video about the issue category, and other educational resources. This section is powered by Secure Code Warrior.

History

The **History** tab displays a log of the following issue events: audit changes, comments, and system events (status changes, copy state actions). You can filter the log by the event type (audit or comment). You can also refresh the history to fetch the latest events.

Auditing multiple issues

You can select multiple issues in an application release and bulk audit multiple issues.

To bulk audit multiple issues:

1. Select an application release.
2. In **REMEDIATE** section, select the check boxes next to the issues.

   The Fortify Code Security Plugin for JetBrains IDE Tools displays the selected issues under the **Selected Issues** area in the **Fortify Issues** panel.

   The **Selected Issues** area displays the total number of selected issues, issue ID, release, and primary location.
3. Click an issue ID under the **Issue ID** column to view the audit information, analysis trace, vulnerability, recommendations, and history for each individual issue.

4. Click the **Multi Selection** button to navigate to the previous page.
5. In the audit panel, edit the fields as needed. The following fields are available for editing: **Assigned User, Developer Status, Auditor, Status, Severity, and Comments.**
6. Click **Save**.

Auto-remediating your code

Use the **Auto Remediate** step in a Fortify on Demand workflow to apply Fortify Remediation Aviator remediation guidance directly to the source code in your current workspace.

This workflow is intended for Fortify on Demand application releases that already contain a Fortify Remediation Aviator-processed artifact.

When you run the Auto Remediate step, the extension uses `fcli fod aviator apply-remediations` in the background to retrieve the artifact and apply the available code changes directly to the local source directory.

Requirements

Before you begin, make sure that the following requirements are met:

- An active Fortify on Demand session exists.
- A workspace folder that contains the application source code is open in IDE.
- A Fortify on Demand application release has already been selected in the sidebar.
- Already performed the Fortify Remediation Aviator audit on the selected application version.

Perform auto-remediation

To auto-remediate vulnerabilities in a Fortify on Demand application release:

1. In the extension sidebar, complete the Fortify on Demand workflow steps to log in and select the target application version.
2. In the sidebar, select **AUTO REMEDIATE**.
3. Click **Auto Remediate** to apply the remediations directly to the local source files for the selected application release.

Review the updated source files and inspect the generated difference in a version control system before committing the changes. After the changes are committed, you can review and test the code, then run another scan to verify that the vulnerabilities were resolved.

If no Fortify Remediation Aviator remediation data is available or if the selected artifact is not eligible for auto-remediation, the extension shows an error or informational message so that you can correct the prerequisite and try again.
Auto-remediation availability depends on Fortify Remediation Aviator support for the language, file type, and vulnerability category in the analyzed artifact. You must review the generated changes before committing them to your code base.

1.4. Using Fortify Code Security Plugin with Application Security Center

This section describes the requirements, configuration, and procedure to use OpenText SAST and ScanCentral SAST to analyze and remediate your code.

With the Fortify Security Code Plugin, you can either:

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

  Note
  You must have a locally installed and licensed OpenText SAST to perform the translation phase.
  OpenText strongly recommends that you periodically update the security content.

- Review and audit issues from Application Security Center and remediate the issues.
- Auto-remediate the issues using Fortify Remediation Aviator recommendations

Requirements

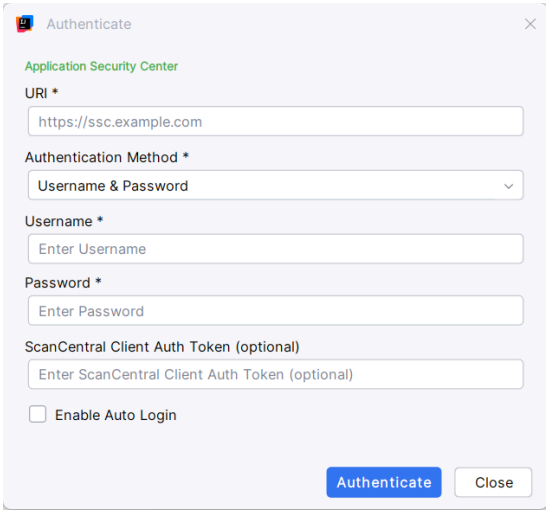
- A locally installed and licensed OpenText SAST with Application Security Content to run local SAST translations and scans.
- A properly configured ScanCentral SAST installation or use the **Install/update ScanCentral Client** settings to install or update the ScanCentral client. For more information, see the *OpenText™ ScanCentral SAST Installation, Configuration, and Usage Guide* in OpenText Application Security Center Documentation.
- An Application Security Center URL and user credentials or an authentication token of type `ToolsConnectToken` or `CIToken`.
- (Optional) A ScanCentral client authentication token to run remote translations or scans.
- The **Preferred Platform** property must be set to Application Security Center (SSC) in the IDE plugin settings.
- The **SAST Executable Path** must be configured for local SAST scans.

- The **Scancentral Client Executable Path** or **ScanCentral Client Version** must be configured to perform remote scans with ScanCentral SAST.

Authenticate your Application Security Center account

1. If the plugin is not open, click **Fortify Code Security** in the tool windows.
2. Click **AUTHENTICATE** in the sidebar.

   The Authenticate box displays.



3. In the **Application Security Center URI** box, type the URL for your Application Security Center server.
4. Select an authentication method and provide the relevant credentials described in the following table.

Authentication Method	Procedure
Username & Password	1. In the **Username** box, type the account username. 2. In the **Password** box, type the account password. 3. (Optiona) In the **ScanCentral Client Auth Token**, type the ScanCentral client authentication token.
Authentication Token	1. In the **ToolsConnect / CI Token** box, type the Application Security authentication token of type `ToolsConnectToken` or `CIToken`. 2. (Optional)In the **ScanCentral Client Auth Token** box, type the ScanCentral client authentication token.

5. (Optional) Select the **Enable Auto Login** check box to securely store credentials and automatically restore expired sessions or silently reauthenticate when a session is missing or expired. No login prompts are displayed.
6. Click **Authenticate**.

   Upon successful authentication, `Authenticated successfully` status is displayed. Otherwise, the status displays `Not Authenticated`.

   To modify the Application Security Center URI, authentication method, or credentials, click **AUTHENTICATE** again.

Select Application and Version

1. Click **SELECT APPLICATION** in the sidebar.
2. In the **Select Application** area, select an application from the **Application Name** list.

> **Note**
> Only 50 entries are displayed in the **Application Name** list.
> When you search for an application, the plugin searches only within these initial 50 entries.
> To view and search additional entries, click **Load next 50 applications...** to load the next set of 50, and repeat as needed.

3. Select a version from the **Version** list.

> **Note**
> Only 50 entries are displayed in the **Version** list. To view additional entries, click **Load next 50 versions...** to load the next set of 50, and repeat as needed.

4. Alternatively, to create a new application or version or modify an existing application or version:
    1. Click + **Create/Modify Application**.

       The **CREATE / MODIFY APPLICATION & VERSION** panel displays in the IDE editor.

    2. Define the application and version. Fields are required, unless otherwise noted.

Field	Description
Application Name	Type the application name or use the **Select an existing application** check box to modify an existing application.
Select an existing application	(Optional) To modify an existing application, select the check box. Select or search for an application from the **Application Name** list.
Version Name	Type a name of the version.
Select an existing version	(Optional) If you have selected the **Select an existing application** check box, you can use the **Select an existing version** check box to modify an existing version. Select or search for a release from the **Version Name** list. When you select a version, the application version attribute values are synced from Application Security Center and populated in the respective fields.
Application Version Attributes	
Development Phase	Current phase of development the application version is in.
Development Strategy	Staffing strategy used for application development.

Field	Description
Accessibility	Level of access required to use the application.
Issue Template	Select the check box for a template that sets the minimum thresholds for issue detection. The default template is Prioritized High Risk Issue Template.

3. Click **Save** to save the application version. The application name and version is displayed in the sidebar.

- Click **Select Application.**

  Upon successful completion, the application name and version is displayed in the sidebar. Click **APPLICATION** again to change the selected application or version.

This section contains the following topics:

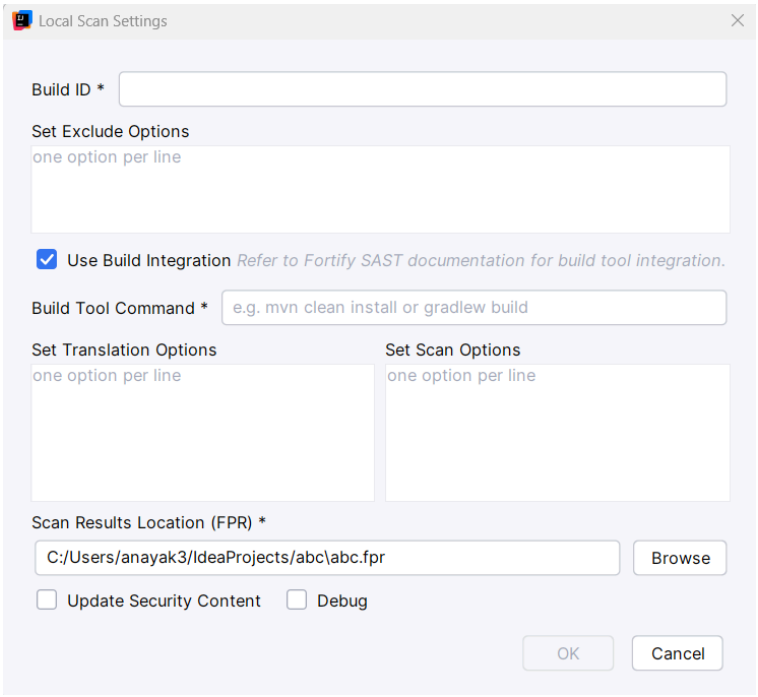
- Performing a local analysis with OpenText SAST
- Performing an analysis remotely with ScanCentral SAST
- Remediate your code in Application Security Center
- Auto-remediate your code in Application Security Center

1.4.1. Performing a local analysis with OpenText SAST

Configuring a local analysis with Fortify SAST

To scan the opened project locally with Fortify SAST:

1. Click **START SCAN** in the sidebar.
2. In the **Scan Type** area, select **Local (SAST)**.
3. In the **LOCAL SCAN OPTIONS** area, click **View/Edit**.



4. Provide the information described in the following table.

Option	Description
Build ID	Required. Type a unique identifier for the analysis.
Use Build Integration	Optional. Enable this option to let Fortify SAST translate the project using build integration whenever a supported build tool integration is available (such as Maven, Gradle, MSBuild/Visual Studio, Make, Xcodebuild, Ant, Bazel). Fortify SAST starts a build integration that analyzes your solution and project files and automatically executes the appropriate translation steps. For more information, see *Fortify SAST User Guide*.
Build Tool Command	Required when **Use Build Integration** is enabled. Type the exact build command you would normally run from the command line to build the project. **Example** mvn clean install gradlew build msbuild MySolution.sln If not specified, the default build command is used.
Set Exclude Options	Optional. Specify the relative paths of files or directories to exclude from the package separated by a new line (one per line). You can use wildcard characters to specify the paths.

Option	Description
Set Translation Options	Optional. Specify a list of Fortify SAST translation options separated by a new line (one per line).
Set Scan Options	Optional. Specify a list of Fortify SAST scan options separated by a new line (one per line).
Scan Results Location (FPR)	Required. Click **Browse** and select the directory where you want to store the scan results file. By default, the plugin stores the scan results file in the current workspace.
Update Security Content	Optional. Enable this option to download Fortify security content before the scan.
Debug	Optional. Select this option to display debug information that can be helpful to troubleshoot issues.

5. Click **Save**.
6. (Optional) To upload results to Application Security, turn on the **Upload Local Scan results to Application Security Center** switch.
7. Click **Start Scan**.

   Fortify Code Security Plugin for JetBrains IDE Tools automatically detects the OpenText SAST path from the IDE plugin settings.

   Fortify Code Security Plugin for JetBrains IDE Tools starts the scan and displays the status information in the Status bar. When the scan is complete, Fortify Code Security Plugin for JetBrains IDE Tools displays the scan completion status in an information message.

1.4.2. Performing an analysis remotely with ScanCentral SAST

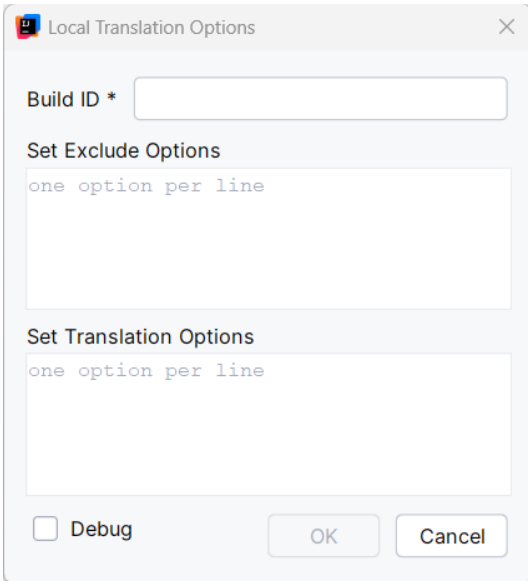
To upload the opened project for analysis by ScanCentral SAST:

1. Click **START SCAN** in the sidebar.
2. In the **Scan Type** area, select **Remote (ScanCentral SAST)**.

Configuring a remote scan with local translation

1. Select **Remote (ScanCentral SAST) > Local Translation** to run the translation phase on the local system and the scan phase with ScanCentral SAST.
2. In the **LOCAL TRANSLATION OPTIONS** area, click **View/Edit**.

   The Local Translation Options dialog box is displayed.



3. Complete the fields as needed.

Option	Description
Build ID	Type a unique identifier for the analysis.
Set Exclude Options	Specify the relative paths of files or directories to exclude from the package separated by a new line (one per line). You can use wildcard characters to specify the paths.
Set Translation Options	Specify a list of OpenText SAST translation options separated by a new line (one per line).
Debug	Select this option to set the log level to contain debug information that can be helpful to troubleshoot issues.

4. Click **OK**.
5. (Optional) In the **REMOTE SCAN OPTIONS** area, click **View/Edit**.

   The Remote Scan Options dialog box is displayed.
6. In the **Scan Options** field, specify a list of ScanCentral SAST scan options separated by a new line (one per line).
7. Click **OK**.
8. Click **Start Scan**.

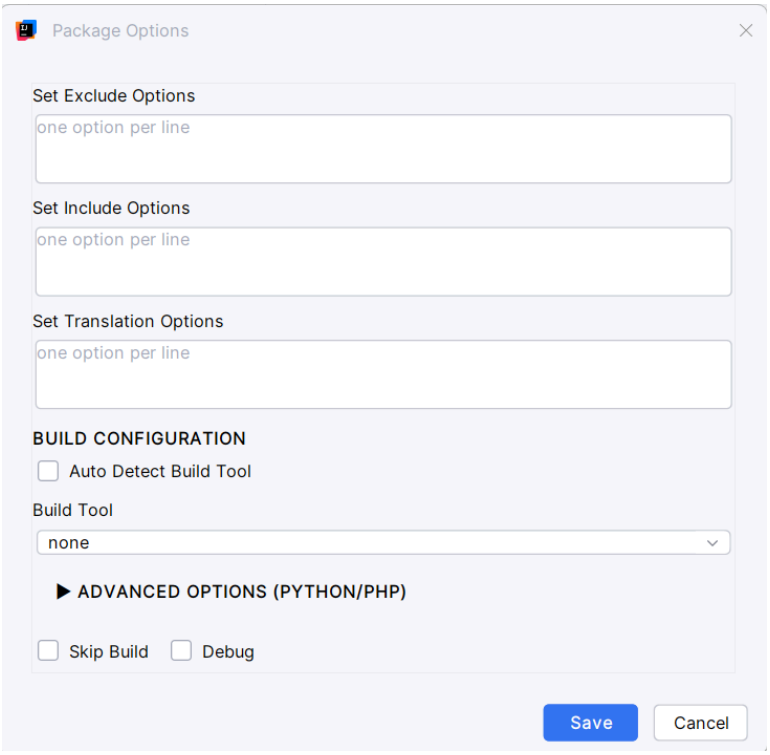
   Fortify Code Security Plugin for JetBrains IDE Tools automatically detects the file path to ScanCentral SAST client executable and the locally installed OpenText SAST executable from the IDE plugin settings.

   Fortify Code Security Plugin for JetBrains IDE Tools starts the scan and displays the status information in the **Status** bar. When the scan is complete, Fortify Code Security Plugin for JetBrains IDE Tools displays the scan completion status and the Job ID in an information message.

Configuring a remote translation and scan

1. Select **Remote (ScanCentral SAST) > Remote Translation** to run the translation phase and the scan phase with ScanCentral SAST.
2. In the **PACKAGE OPTIONS** area, click **View/Edit**.

   The Package Options box is displayed.



3. Provide the options described in the following table. All field are optional, unless otherwise noted.

Option	Description
Set Exclude Options	Specify the relative paths of files or directories to exclude from the package separated by a new line (one per line). You can use wildcard characters to specify the paths.
Set Include Options	Specify the relative paths of files or directories to include in the package separated by a new line (one per line). You can use wildcard characters to specify the paths. If you leave it empty, all the supported files are included.
Set Translation Options	Specify a list of OpenText SAST translation options separated by a new line (one per line).

Option	Description
Auto Detect Build Tool	Select this option to automatically detect the build tool. **Note** For .NET projects: ◦ On Windows, if you select the **Auto Detect build tool** option, the default build tool is MSBuild. ◦ On Linux, if you select the **Auto Detect build tool** option, the default build tool is DotNet. ◦ If you want to use DotNet as the build tool on a Windows, you must clear the **Auto Detect build tool** option and explicitly select **DotNet** from the **Build Tool** list.
Skip Build	Select whether to skip the build invocation that prepares the generated sources and libraries before the project information is packaged for submission to ScanCentral SAST.
Set Debug	Select this option to display debug information that can be helpful to troubleshoot issues.

4. To select a build tool explicitly, clear the **Auto Detect build tool** option. The **Build Tool** list is displayed.

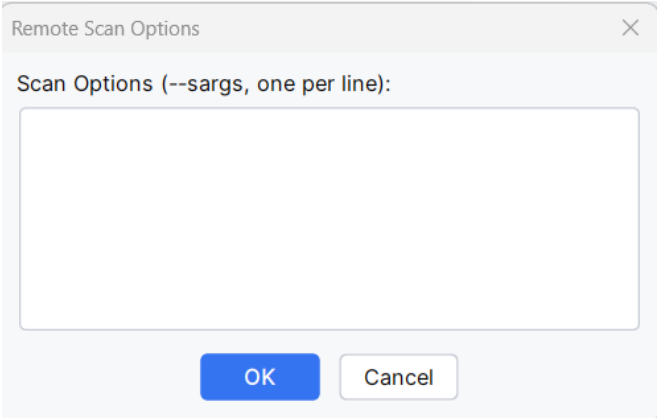
5. Select the build tool in the **Build Tool** list and provide the settings based on the build tool.

Option	Description
Build File	(Optional) (For Gradle or Maven) Click **Browse** and select the build file if it is different than the default of `build.gradle` or `pom.xml`. (For DotNet or MSBuild) Type the name of the build file. If you do not select a build file, ScanCentral SAST automatically detects the build file.
Build Command	(Optional) Type any custom build commands to prepare and build the project. If not specified, the default build command is used.
Advanced Options (Python/PHP) (applies only when you select None in the Build Tool list)	
PHP Version	(Optional) Type the PHP version used in the project.
Python Virtual Environment Location	(Optional) Click **Browse** and select the location (directory) of the Python virtual environment. Specify this together with the Python requirements file to have dependencies restored before the scan.

Option	Description
Python Requirements File	(Optional) Click **Browse** and select the Python project requirements file used to install and collect dependencies. Use only this Python field if you have no preference for the Python version used or there is only one Python version installed and on the PATH.
Python Version	(Optional) Select the Python version for Python projects.

6. Click **Save**.
7. (Optional) In the **Remote Scan Options** area, click **View/Edit**.

   The **Remote Scan Options** box is displayed in the VS Code editor.



8. In the **Set Scan Options** field, specify a list of ScanCentral SAST scan options separated by a new line (one per line).
9. Click **Save**.
10. Click **Start Scan**.

    Fortify Code Security Plugin for JetBrains IDE Tools automatically detects the file path to ScanCentral SAST client executable from the IDE plugin settings.

    Fortify Code Security Plugin for JetBrains IDE Tools starts the scan and displays the status information in Status bar. When the scan is complete, Fortify Code Security Plugin for JetBrains IDE Tools displays the scan completion status and the Job ID in an information message.

1.4.3. Remediate your code in Application Security Center

After you select an application version, you can view and audit the scan results and remediate issues found in your application.

Viewing and selecting issues

To view and select issues in an opened application **version**:

1. Click **REMEDIATE** in the sidebar.

   From the **GroupBy** list, select an attribute for sorting issues in all visible folders into groups. The default grouping is Category.

2. Click a tab grouped by issue severity to view the associated issues.
   - The **Critical** tab contains issues that have a high impact and a high likelihood of exploitation. We recommend that you remediate critical issues immediately.
   - The **High** tab contains issues that have a high impact and a low likelihood of exploitation. We recommend 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. We recommend that you remediate medium issues as time permits.
   - The **Low** tab contains issues that have a low impact and a low likelihood of exploitation. We recommend that you remediate low issues as time permits (your organization can customize this category).
   - The **All** tab contains all issues.

   Within each tab, issues are grouped by issue category. After each grouping name, enclosed in brackets, is the number of audited issues and the total number of issues in the group.

3. To view removed and/or suppressed issues,
   click **Removed** and/or **Suppressed** from the **Visibility** list.

4. Click to expand a grouping and view the issues it contains.

   The Fortify Code Security Plugin for JetBrains IDE Tools retrieves the corresponding issues from Application Security Center.

5. Select an issue to view its details in the **ISSUE AUDIT** panel.

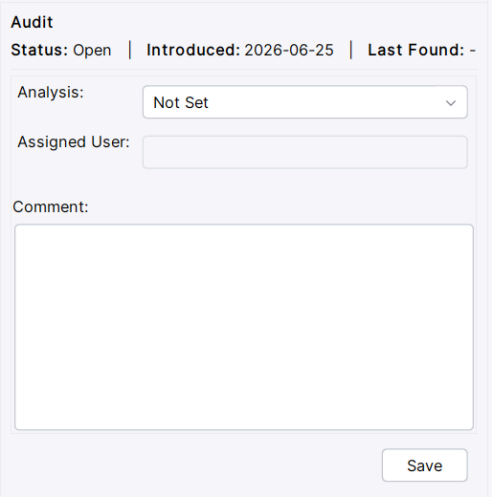
6. Click the **Refresh** icon to sync any changes to the issues in the application version in Application Security.

Viewing issue information

After you select an issue in the **ISSUE AUDIT** panel, the Fortify Code Security Plugin for JetBrains IDE Tools displays the issue-specific content in the in the **ISSUE AUDIT** panel on the **Audit**, **Analysis Trace**, **Vulnerablity**, **Recommendations**, and **History** tabs.

Auditing issues

The **AUDIT** view provides a dashboard of analysis information for the selected issue.



To audit an issue:

1. Make sure that the **Audit** view is open.
2. From the issues list in the **REMEDIATE** section, select an issue. You can select multiple issues to make the same edits to multiple issues.
3. In the **Audit** view, select the user to assign to the issue from **User** list.
4. To change the analysis status, select the status from the **Analysis** list.
5. To add a comment for the issue, type your comment in the box at the bottom of the **Comments** area..
6. Click **Save**.

   The changes and comments are displayed in the **History** tab.

The Fortify Code Security Plugin for JetBrains IDE Tools saves your changes for the selected application version.
Any changes you make on the **Audit** tab are automatically uploaded to the application version in Application Security Center.

Grouping issues

The following grouping options are available on the **REMEDIATE** section:

Group	Description
Analysis	Issues that have the specified audit analysis value such as `exploitable`, `not an issue`, and so on.
Analysis type	Issues based on the analyzer product.
Analyzer	Issues for the specified analyzer such as `control flow`, `data flow`, `structural`, and so on.
App Defender Protected	App Defender Protected issues.
Audience	Issues by intended audience.
Audited	Issues to find `true` if the primary custom tag is set and `false` if the primary custom tag is not set. The default primary tag is the Analysis tag.
Category	The given category or category substring.
Engine Priority	issues based on the original priority value determined by the engine that identified the issue.
File Name	Issues where the primary location or sink node function call occurs in the specified file.
Folder	Issues based on their assignment to a Fortify folder.

Group	Description
Fortify Priority Order	Issues that have a priority level that matches the specified priority.
Issue State	The issue state, which is `new`, `updated`, `reintroduced`, or `removed`.
Kingdom	All issues in the specified kingdom.
Manual	
<metadata_listname>	Issues with the specified metadata external list. Metadata external lists include `[OWASP top ten <year>]`, `[CWE top 25 <version>]`, `[stig <version>]`, and `[pci ssf <version>]`, and others.
Package	Issues where the primary location occurs in the specified package or namespace. For dataflow issues, the primary location is the sink function.
Primary Context	Issues where the primary location or sink node function call occurs in the specified code context.
Priority Override	Issues with overridden priorities, grouped by the priority override tag value. Issues with unchanged priority values are grouped under **Not Set**.

Group	Description
Sink	Issues that have the specified sink function name.
Source	Dataflow issues that have the specified source function name.
Source Context	Dataflow issues that have the source function call contained in the specified code context
Source File	Dataflow issues with the source function call that the specified file contains.
Status	Issues that have the status reviewed, not reviewed, or under review.
Taint Flag	Issues that have the specified taint flag.

Analysis Trace

The **Analysis Trace** tab displays the relevant trace output. This is a set of program points that show how the analyzer found the issue. VS Code places the focus on the line of code that contains the selected security-related issue.

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 box shows the direction of the dataflow in this section of the source code.

Analysis Trace Icons

The analysis trace icons described in the following table show how dataflow moves in the section of the source code or execution order.

Icon	Description	Icon	Description
	Data is assigned to a field or variable		Tainted data is returned from a function
	Information is read from a source external to the code such as an HTML form or a URL		A pointer is created
	Data is assigned to a globally scoped field or variable		A pointer is dereferenced
	A comparison is made		The scope of a variable ends
	The function call receives tainted data		The execution jumps
	The function call returns tainted data		A branch is taken in the code execution

Icon	Description	Icon	Description
	Passthrough, tainted data passes from one place to another This is typically shown as functionA(x : y) to indicate that data is transferred from x to y. The x and y values are one of the following: • An argument index • `return` —The return value of a function • `this` —The instance of the current object • A specific object field or key		A branch is not taken in the code execution
	An alias is created for a memory location		Generic

Icon	Description	Icon	Description
	Data is read from a variable		A runtime source, sink, or validation step
	Data is read from a global variable		Taint change

Vulnerability

The **Vulnerability** tab displays the following technical details about the issue:

- Issue summary
- Issue overview
- Issue name
- Function
- File name and path
- Instance ID and primary rule GUID
- Package name
- Probability
- References
- Link to Secure Code Warrior Training Portal

1.4.4. Auto-remediate your code in Application Security Center

Use the **AUTO REMEDIATE** step in an Application Security Center workflow to apply Fortify Remediation Aviator remediation guidance directly to the source code in your current workspace.

> **Note**
> This workflow is intended for Application Security Center application versions that already contain a Fortify Remediation Aviator-processed artifact.

When you run the **AUTO REMEDIATE** step, the extension uses `fcli aviator ssc apply-remediations` in the background to retrieve the artifact and apply the available code changes directly to the local source directory.

Requirements

Before you begin, make sure that the following requirements are met:

- An active Application Security Center session exists.
- A workspace folder that contains the application source code is open in IntelliJ IDEA.
- An Application Security Center application version has already been selected in the sidebar.
- Already performed the Foritfy Remediation Aviator audit on the selected application version.

Perform auto-remediation

To auto-remediate vulnerabilities in an Application Security Center application version:

1. In the plugin sidebar, complete the Application Security Center workflow steps to log in and select the target application version.
2. In the sidebar, select **AUTO REMEDIATE**.
3. Click **Aviator Authentication** to authenticate your Application Security Center Aviator account and provide the relevant credentials described in the following table.

Field	Description
Aviator URL	(Required) Specifies the Fortify Remediation Aviator server URL.
User Access Token	(Required) Specifies the Fortify Remediation Aviator personal access token for the user.

4. Click **Authenticate**.

   Upon successful authentication, **Authenticated** status is displayed. Otherwise, the status displays **Not Authenticated**.

   The **Aviator Authentication** remains valid even if you restart the plugin or IDE and remains active until the session expires.

5. (Optional) Select the **Run Audit before Remediation** check box to trigger a Fortify Remediation Aviator audit in an application.

   Recommendation

   Select this option when you want remediation recommendations to be based on the most recent scanned version of the code, rather than using a previously audited artifact.
   - When enabled, the extension runs a Fortify Remediation Aviator audit for the selected Application Security Center application version, waits for the audited artifact to become available, and then applies the remediation suggestions.
   - When disabled, the extension skips the audit step and applies remediations from the most recent eligible Fortify Remediation Aviator–processed artifact already available in Application Security Center. This option completes faster, but the remediation suggestions may be based on an older scan context.

6. (Required when you select **Run Audit before Remediation**) Specify the target application name in Fortify Remediation Aviator in the **Aviator Application Name** box.

> **Note**
> The **Aviator Application Name** identifies the target application in Fortify Remediation Aviator that is used for the audit and remediation workflow.
> If the name is incorrect or does not exist in Fortify Remediation Aviator, the workflow can fail during audit or remediation retrieval, so verify the exact Fortify Remediation Aviator application name before running.

7. Click **Auto Remediate** to apply the remediations directly to the local source files for the selected application version.

> **Tip**
> Review the updated source files and inspect the generated difference in a version control system before committing the changes. After the changes are committed, you can review and test the code, then run another scan to verify that the vulnerabilities were resolved.

> **Note**
> If no Fortify Remediation Aviator remediation data is available or if the selected artifact is not eligible for auto-remediation, the extension shows an error or informational message so that you can correct the prerequisite and try again.
> Auto-remediation availability depends on Fortify Remediation Aviator support for the language, file type, and vulnerability category in the analyzed artifact. You must review the generated changes before committing them to your code base.

1.5. Using FCli: Discover Resources and Commands

The plugin uses fcli as a unified command-line interface to work with both Fortify on Demand and Application Security (Software Security Center). Instead of handling platform-specific behavior within the plugin, fcli provides a consistent command set by abstracting platform differences such as authentication, application structure, and scan submission.

When you set the preferred platform in the plugin settings, the plugin automatically invokes the corresponding fcli module (fod or ssc). Session handling is managed automatically and results are normalized so that scanning, issue retrieval, and remediation workflows behave consistently, regardless of the selected platform.

Discover commands dynamically

Use `FCli: Discover Resources and Commands` to view the parameters and options supported by your installed fcli version, rather than entering commands manually.

When you click `FCli: Discover Resources and Commands`:

- The plugin queries fcli for all available commands for the preferred platform.
- fcli returns platform-specific commands, parameters, and valid options in JSON-RPC format.
- Use the **Execute via Dialog** window to specify command parameters in a form. The commands to execute are automatically updated as you specify the command parameters in the form.

Example

For Fortify on Demand, fcli exposes commands such as:

- `fcli fod sast-scan start` : Submit a remote SAST scan
- `fcli fod issue list` : Retrieve vulnerabilities
- `fcli fod release get` : Fetch release details

Example

For Application Security Center, fcli exposes command such as:

- `fcli ssc artifact upload` : Upload scan results
- `fcli ssc issue list` : Retrieve vulnerabilities
- `fcli ssc appversion get` : Fetch application version details

Saved configuration in Favorites

Use the **Favorites** section to save and reuse command configurations for recurring workflows.

1. Open the **Fortify Code Security** activity bar view.
2. Press **Ctrl+Shift+A** (**Find Action**).
3. In the search box, type **FCli: Discover Resources and Commands**.

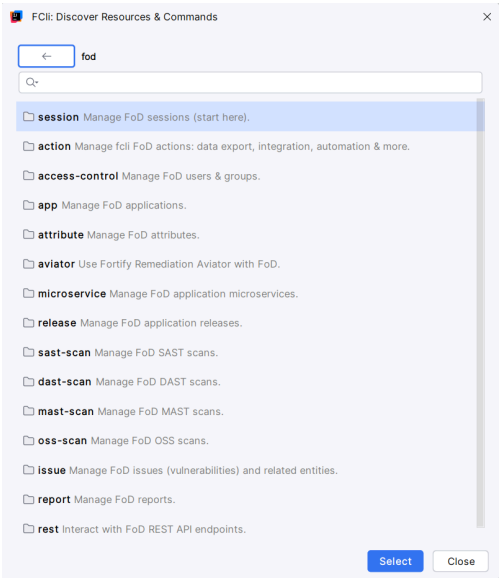
   Based on the preferred platform, fcli displays all the available commands for the platform and categorizes the commands based on the resources.

4. Select a command from the list.
5. fcli opens **Execute via Dialog** window for the base fcli command you want to save.
6. Edit the parameters in the dialog box.
7. Select **Save Configuration**.
8. Enter a configuration name in the Save Configuration dialog box.
9. Press **OK** to confirm.
10. Expand **Favorites** in the sidebar. The configuration is saved under the folder name corresponding to the base fcli command.
11. Select the saved configuration.
12. Run, update, rename, or delete the saved configuration using inline actions.

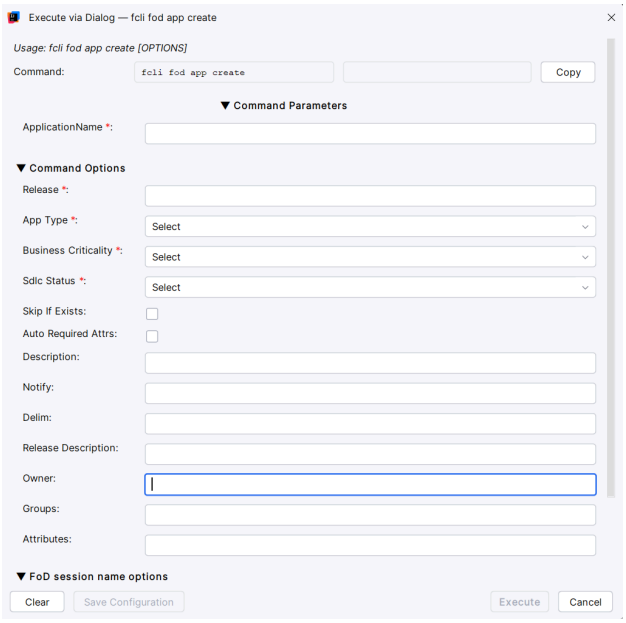
Example: Creating a Fortify on Demand application

1. Open the **Fortify Code Security** activity bar view.
2. In the **Plugin Settings**, select **Fortify on Demand (FoD)** as the **Preferred Platform**.
3. Press **Ctrl+Shift+A** (**Find Action**).
4. In the search box, type **FCli: Discover Resources and Commands**.
5. Select **FCli: Discover Resources and Commands > fod**

   fcli displays all the available commands for Fortify on Demand and categorizes the commands based on the resources.



6. Select **app > fcli fod app create** to create a new application.
7. fcli displays the form for `fcli fod app create` in the **Execute via Dialog** window.



8. Specify the Application Name in the **Command Parameters** area.
9. Specify the Release, App Type, Business Criticality, Sdlc Status, and other advanced options in the **Command Options** area.

   When you edit a parameter or option, fcli automatically updates the command that will be executed in the **Commands to execute** area for `fcli fod app create`. You can copy the full command to run a direct command.
10. Click **Execute** to run the command.
11. (Optional) Click **Save Configuration** to save the configuration in **Favourites** in the plugin sidebar.

When you run the command, fcli sends a request to create the application in your Fortify on Demand tenant. The confirmation message is displayed in the Status bar indicating that the application release were created successfully.

The new application is immediately available in your Fortify on Demand instance and appears in the plugin during the **SELECT APPLICATION** step. You can then select it to start **START SCAN** or **REMEDIATE** workflows. If a validation error occurs, such as a duplicate application name or insufficient permissions, fcli displays an error message in the Notifications so you can correct the issue and try again.

1.6. Using JetBrains AI Assistant with the Fortify Code Security Plugin

Use JetBrains AI Assistant with the Fortify Code Security Plugin for JetBrains IDE Tools to investigate findings, retrieve vulnerability data from Fortify platforms, and accelerate remediation decisions from inside the JetBrains IDE.

Requirements

Before using JetBrains AI Assistant for Fortify tasks, you must meet the following requirements:

- JetBrains AI Assistant is enabled in the JetBrains IDE.
- The plugin is configured with a valid fcli executable path.
- You are logged in to Fortify on Demand or Application Security Center.
- Enable MCP Server in **Settings > Tools > MCP Server**.
- Set the **Pass IntelliJ MCP Server** to **On** or **On demand** in **Settings > Tools > AI Assistant > Agents > Pass IntelliJ MCP Server**
- The **FortifyCodeSecurityToolset** is enabled in **Settings > Tools > MCP Server > Exposed Tools**.

Exposed Fortify MCP servers

The following Fortify MCP servers are registered by the plugin and exposed to JetBrains AI Assistant. Each Fortify MCP server can be individually enabled or disabled in **Settings > Tools > AI Assistant > Model Context Protocol (MCP)**.

Fortify MCP server	Usage
Fortify-Core-Application-Security	Use this when you use Fortify on Demand and you want AI Assistant to browse applications/releases, start scans, or remediate and audit issues.
Fortify-Application-Security-Centre	Use this when you use Application Security Center and you want AI Assistant to manage applications/versions, upload scan results, or remediate and audit issues.
Fortify-Aviator	Use this when you want AI Assistant to request Fortify Remediation Aviator remediation fixes for issues, or to manage Fortify Remediation Aviator entitlements, independent of which platform (FoD/SSC) hosts the issue.
Fortify-Scan-Central-SAST	Use this when you want AI Assistant to start a remote ScanCentral SAST scan, list ScanCentral jobs, sensors, and sensor pools, download ScanCentral SAST job artifacts.
Fortify-Scan-Central-DAST	Use this when you want AI Assistant to configure, start, or check the status of a ScanCentral DAST scan against a running application.

Enabling / Disabling a Fortify MCP Server

1. Click **Settings > Tools > AI Assistant > Model Context Protocol (MCP)**.
2. Use the checkbox next to a server name to enable/disable it without deleting its configuration.
3. The green check under Status confirms the server process started successfully.
4. Click a row's expand arrow to inspect the fcli commands or use the toolbar icons (+, pencil, up/down arrows, refresh) to add, remove, edit, reorder, or restart a server.

Exposed Fortify MCP tools

The following tools are registered by the plugin and exposed to JetBrains MCP server. Each tool can be individually enabled or disabled in **Settings > Tools > MCP Server > Exposed Tools**.

Tool	Description
get_vulnerabilities	Displays the vulnerability or issue list for an application version or release from the connected platform in the **REMEDIATE** section. You can optionally filter by severity, issue category, or auditing status (including suppressed issues). AI Assistant uses the results to provide analysis, prioritization guidance, and remediation suggestions. If there are no active sessions, AI Assistant prompts you to login via the Authenticate window. Use this tool when you want to query existing findings and get AI-assisted prioritization or explanations.
search_app	Searches for an application by name keyword and, optionally, resolves one of its versions (SSC) or releases (FoD). AI Assistant uses this tool automatically when a prompt refers to an application by name so it can look up the correct identifier before fetching findings. Use this tool when you want to browse available applications on the platform, select an application release/version in the APPLICATION step of the workflow, or let AI Assistant resolve an application name before performing further operations.

Enable Fortify MCP tools

1. Click **Settings > Tools > MCP Server**.
2. Select the **Enable MCP Server** check box.
3. Go to **Settings > Tools > MCP Server > Exposed Tools**.
4. Locate **FortifyCodeSecurityToolset** and select the check box to enable it.
5. Ensure the following tools are selected:
    - **get_vulnerabilities**: Fetches vulnerabilities for an application version from Fortify on Demand or Application Security Center.
    - **search_app**: Searches for an application and, optionally, one of its Fortify on Demand releases or Application Security Center versions by keyword.

    > **Note**
    > Enable only the tools relevant to your current task. Enabling unnecessary tools can reduce accuracy.

6. Click **OK** to apply.

Exposed Fortify Skills

The plugin installs the following Fortify skills in the JetBrains AI Assistant in **Settings > Tools > AI Assistant > Skills**:

Skills	Usage
fcli-common	Generic reference for the Fortify CLI (fcli). Install, upgrade, authenticate, fcli environment variables, output formats, SpEL query syntax, variable chaining and custom action framework.
fortify-change-review	Lightweight, AI-powered security review of code changes such as a diff, PR, or in-session edits.
fortify-cicd-integration	Integrates Fortify application security (SAST, SCA, DAST) with GitHub Actions, GitLab Pipelines, Azure DevOps, Jenkins & other CICD/DevSecOps pipelines.
fortify-create-app	Create new Fortify application(s) in Fortify on Demand (FoD) or Application Security Center (SSC).
fortify-fod	Query, scan, and audit in Fortify on Demand.
fortify-ssc	Query, scan, and triage in Application Security Center.
fortify-remediate	Fix SAST issues already found by Fortify in Fortify on Demand or Application Security Center.
fortify-dependency-upgrade	Upgrade a vulnerable dependency safely, with full impact analysis
fortify-exploitability-analysis	Find out if a CVE actually affects your code before you act on it

Tip

fcli dynamically updates the Fortify skills or adds new skills. Restart the IDE to expose the latest skills to AI Assistant.

JetBrains AI Chat usage

Once the FortifyCodeSecurityToolset is enabled, JetBrains AI Assistant can invoke Fortify tools automatically based on your prompts.

There are no chat participants to prefix. Type your request directly in the JetBrains AI Chat.

Recommendation

Recommended usage pattern:

- Use / to invoke a specific Fortify MCP server or skills based on your prompts.
- Use AI Assistant chat to retrieve current findings for the target SSC version or FoD release.
- Ask AI Assistant to explain specific issues and suggest remediation approaches.
- Apply code fixes in the workspace and validate with your normal build and test process.
- Re-run analysis to confirm the issues are resolved.

Example

You can use prompts such as:

- Show High and Critical vulnerabilities for Payments:main in SSC.
- List SQL Injection issues for the RetailBank release main in FoD.
- Get vulnerabilities for the currently selected application version and include suppressed issues.
- What should I fix first and why for this application version?
- Start a scan for the current project against SSC.

1.7. Using GitHub Copilot with the Fortify Code Security Plugin

Use GitHub Copilot with the Fortify Code Security Plugin for IntelliJ IDEA and Android Studio to investigate findings, retrieve vulnerability data from Fortify platforms, and accelerate remediation decisions from inside the JetBrains IDE.

Requirements

Before using GitHub Copilot for Fortify tasks, you must meet the following requirements:

- GitHub Copilot is enabled in the JetBrains IDE.
- The plugin is configured with a valid fcli executable path.
- You are logged in to OpenText Core Application Security or Application Security Center.
- Enable MCP Server in **Settings > Tools > MCP Server**.
- Set the **Pass IntelliJ MCP Server** to **On** or **On demand** in **Settings > Tools > GitHub Copilot > Agents > Pass IntelliJ MCP Server**
- The **FortifyCodeSecurityToolset** is enabled in **Settings > Tools > MCP Server > Exposed Tools**.

Exposed Fortify MCP servers

The following Fortify MCP servers are registered by the plugin and exposed to GitHub Copilot. Each Fortify MCP server can be individually enabled or disabled in **Chat Settings > Customizations > MCP Servers**.

Fortify MCP server	Usage
Fortify-Core-Application-Security	Use this when you use Fortify on Demand and you want GitHub Copilot to browse applications/releases, start scans, or remediate and audit issues.
Fortify-Application-Security-Centre	Use this when you use Application Security Center and you want GitHub Copilot to manage applications/versions, upload scan results, or remediate and audit issues.
Fortify-Aviator	Use this when you want GitHub Copilot to request Fortify Remediation Aviator remediation fixes for issues, or to manage Fortify Remediation Aviator entitlements, independent of which platform (FoD/SSC) hosts the issue.
Fortify-Scan-Central-SAST	Use this when you want GitHub Copilot to start a remote ScanCentral SAST scan, list ScanCentral jobs, sensors, and sensor pools, download ScanCentral SAST job artifacts.
Fortify-Scan-Central-DAST	Use this when you want GitHub Copilot to configure, start, or check the status of a ScanCentral DAST scan against a running application.

Enabling / Disabling a Fortify MCP Server

1. Click **Settings > Tools > GitHub Copilot > Model Context Protocol (MCP)**.
2. Use the checkbox next to a server name to enable/disable it without deleting its configuration.
3. The green check under Status confirms the server process started successfully.
4. Click a row's expand arrow to inspect the fcli commands or use the toolbar icons (+, pencil, up/down arrows, refresh) to add, remove, edit, reorder, or restart a server.

Exposed Fortify MCP tools

The following tools are registered by the plugin and exposed to GitHub Copilot through the MCP server. Each tool can be individually enabled or disabled in **Settings > Tools > MCP Server > Exposed Tools**.

Tool	Description
get_vulnerabilities	Displays the vulnerability or issue list for an application version or release from the connected platform in the **REMEDIATE** section. You can optionally filter by severity, issue category, or auditing status (including suppressed issues). GitHub Copilot uses the results to provide analysis, prioritization guidance, and remediation suggestions. If there are no active sessions, GitHub Copilot prompts you to login via the Authenticate window. Use this tool when you want to query existing findings and get AI-assisted prioritization or explanations.
search_app	Searches for an application by name keyword and, optionally, resolves one of its versions (SSC) or releases (FoD). GitHub Copilot uses this tool automatically when a prompt refers to an application by name so it can look up the correct identifier before fetching findings. Use this tool when you want to browse available applications on the platform, select an application release/version in the APPLICATION step of the workflow, or let GitHub Copilot resolve an application name before performing further operations.

Enable Fortify MCP tools

1. Go to **Settings > Tools > MCP Server**.
2. Select the **Enable MCP Server** check box.
3. Go to **Settings > Tools > MCP Server > Exposed Tools**.
4. Locate **FortifyCodeSecurityToolset** and select the check box to enable it.
5. Ensure the following tools are selected:
    - **get_vulnerabilities**: Fetches vulnerabilities for an application version from OpenText Core Application Security or Application Security Center.
    - **search_app**: Searches for an application and, optionally, one of its OpenText Core Application Security releases or Application Security Center versions by keyword.
      Enable only the tools relevant to your current task. Enabling unnecessary tools can reduce accuracy.
6. Click **OK** to apply.

Exposed Fortify Skills

The plugin installs the following Fortify skills in the GitHub Copilot in **Chat Settings > Customizations > Skills**:

Skills	Usage
fcli-common	Generic reference for the Fortify CLI (fcli). Install, upgrade, authenticate, fcli environment variables, output formats, SpEL query syntax, variable chaining and custom action framework.
fortify-change-review	Lightweight, AI-powered security review of code changes such as a diff, PR, or in-session edits.
fortify-cicd-integration	Integrates Fortify application security (SAST, SCA, DAST) with GitHub Actions, GitLab Pipelines, Azure DevOps, Jenkins & other CICD/DevSecOps pipelines.
fortify-create-app	Create new Fortify application(s) in Fortify on Demand (FoD) or Application Security Center (SSC).
fortify-fod	Query, scan, and audit in Fortify on Demand.
fortify-ssc	Query, scan, and triage in Application Security Center.
fortify-remediate	Fix SAST issues already found by Fortify in Fortify on Demand or Application Security Center.
fortify-dependency-upgrade	Upgrade a vulnerable dependency safely, with full impact analysis
fortify-exploitability-analysis	Find out if a CVE actually affects your code before you act on it

Tip

fcli dynamically updates the Fortify skills or adds new skills. Restart the IDE to expose the latest skills to GitHub Copilot.

GitHubCopilot Chat usage

Once the FortifyCodeSecurityToolset is enabled, GitHub Copilot Chat can invoke Fortify tools automatically based on your prompts.

There are no chat participants to prefix. Type your request directly in the GitHub Copilot Chat.

Recommendation

Recommended usage pattern:

- Use / to invoke a specific Fortify skills based on your prompts.
- Use **Configure Tools** to invoke Fortify MCP servers.
- Use GitHub Copilot Chat to retrieve current findings for the target SSC version or FoD release.
- Ask GitHub Copilot Chat to explain specific issues and suggest remediation approaches.
- Apply code fixes in the workspace and validate with your normal build and test process.
- Re-run analysis to confirm the issues are resolved.

Example

You can use prompts such as:

- Show High and Critical vulnerabilities for Payments:main in SSC.
- List SQL Injection issues for the RetailBank release main in FoD.
- Get vulnerabilities for the currently selected application version and include suppressed issues.
- What should I fix first and why for this application version?
- Start a scan for the current project against SSC.