opentext™

OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studio

Software Version: 24.4.0

User Guide

Document Release Date: October 2024
Software Release Date: October 2024

Legal Notices

Open Text Corporation

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

Copyright Notice

Trademark Notices

Documentation Updates

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

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

This document was produced on September 27, 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

Contacting Customer Support

Visit the Support website to:

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

https://www.microfocus.com/support

For More Information

For more information about Fortify software products:

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

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 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 Fortify Community:

https://community.microfocus.com/cyberres/fortify/w/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.

Software Release / Document Version	Change
24.4.0	Updated: • The **Synchronize Options** tab has been renamed **Server Configuration** (see "Integrating with Fortify Software Security Center" on page 14)
24.2.0	Updated: • The Fortify Analysis Plugin for IntelliJ IDEA and Android Studio is available to install from the JetBrains Marketplace (see "Installing the Fortify Analysis Plugin" on page 8) • Added how to use a standalone Fortify ScanCentral SAST client (see "Requirements for using the Fortify Analysis Plugin" on the next page, "Requirements to scan with Fortify ScanCentral SAST" on page 25, "Configuring Fortify ScanCentral SAST options" on page 26, and "Scanning projects with Fortify ScanCentral SAST" on page 28)
23.2.0	Updated: • Expanded the description for using an SSL connection to Fortify Software Security Center (see "Requirements for using the Fortify Analysis Plugin" on the next page)
23.1.0	Updated: • Changes were made throughout this guide for the introduction of the Fortify Static Code Analyzer Applications and Tools installer • Before you analyze your code, you need to specify the location of the Fortify Static Code Analyzer installation (see "Requirements for using the Fortify Analysis Plugin" on the next page)

Getting started

This guide describes how to install the Fortify Analysis Plugin for IntelliJ IDEA and Android Studio (Fortify Analysis Plugin) and use it to scan your code from the IDE with OpenText™ Fortify Static Code Analyzer.

This section contains the following topics:

About the Fortify Analysis Plugin

The Fortify Analysis Plugin focuses on scanning your project to identify vulnerabilities in the code. You can use the Fortify Analysis Plugin with IntelliJ IDEA and Android Studio.

After you install the Fortify Analysis Plugin, you can:

- Configure your analysis options and then scan your project locally with Fortify Static Code Analyzer or remotely with OpenText™ Fortify ScanCentral SAST.
- Upload the analysis results to OpenText™ Fortify Software Security Center for your organization to manage projects and assign issues to the relevant developers.

Requirements for using the Fortify Analysis Plugin

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

To scan your code, you must have either:

- A locally installed and licensed Fortify Static Code Analyzer with Fortify Software Security Content

  For installation instructions, see the *OpenText™ Fortify Static Code Analyzer User Guide*.

- A local Fortify ScanCentral SAST client and a properly configured Fortify ScanCentral SAST installation

  You can install Fortify ScanCentral SAST client, as a component with either the Fortify Static Code Analyzer or the Fortify Applications and Tools installation or from a Fortify ScanCentral SAST ZIP archive.

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

- The Fortify Software Security Center URL
- A user account with permission to upload to application versions
- If Fortify Software Security Center uses an SSL connection from an internal certificate authority or a self-signed certificate, you must import the certificate into the Java Runtime Environment (JRE) certificate store. See the IntelliJ IDEA or Android Studio documentation for more information. The following is an example of the certificate storage location: `<IDE_install_dir>/jbr/lib/security/cacerts`.

See Also

"About Analyzing the source code" on page 14

Installing the Fortify Analysis Plugin

You can install the Fortify Analysis Plugin on Windows, Linux, and macOS.

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

The Fortify Analysis Plugin is available to install from the JetBrains Marketplace or from the IntelliJ IDEA Analysis component installed with Fortify Applications and Tools.

To install the Fortify Analysis Plugin:

1. Start IntelliJ IDEA or Android Studio.
2. Open the **Settings** or **Preferences**.
3. In the left pane, select **Plugins**.
4. Select the Fortify Analysis Plugin to install by doing one of the following:
   - Install from the JetBrains Marketplace:
     i. Select the **Marketplace** tab, and then in the search box type `Fortify Analysis`.
     ii. Select the Fortify Analysis Plugin, and then click **Install**.
   - Install from the Fortify Applications and Tools installation:
     i. Select **Install Plugin from Disk**.
     ii. Go to `<tools_install_dir>/plugins/IntelliJAnalysis/`, and then select `Fortify_IntelliJ_Analysis_Plugin_<version>.zip`.
5. Click **OK**.
6. To activate the plugin, restart the IDE.

The IDE **Tools** menu now includes the **Fortify** menu.

Fortify Security Content

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

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

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

You must have security content on your local system to run a scan locally or to use Fortify ScanCentral SAST and run the translation locally (see "About Analyzing the source code" on page 14). Typically, you obtain the current Fortify Security Content when you install Fortify Static Code Analyzer. For information about updating Fortify security content, see "Updating Fortify Security Content" below. OpenText strongly recommends that you periodically update the security content.

Updating Fortify Security Content

To update the security content:

1. Open a command prompt, and then go to `<sca_install_dir>/bin/`.
2. Do one of the following:
   - To download and update security content from the Rulepack update server, type `fortifyupdate`.
     If your network uses a proxy server to reach the Rulepack update server, see "Updating Fortify Security Content on a network that uses a proxy server" on the next page.
   - To update the security content from a local ZIP file that contains archived security content, type `fortifyupdate -import <zip_file>`.

Note: You can also use the fortifyupdate command-line tool to update security content from a Fortify Software Security Center server. For instructions, see the *OpenText™ Fortify Static Code Analyzer User Guide*.

Updating Fortify Security Content on a network that uses a proxy server

If your network uses a proxy server to reach the Rulepack update server, you must use the scapostinstall utility to specify the proxy server.

To specify a proxy for the Rulepack update server and download the latest security content:

1. Open a command window, and then go to `<sca_install_dir>/bin/`.
2. At the command prompt, type `scapostinstall`.
3. Type `2` to select `Settings`.
4. Type `2` to select `Fortify Update`.
5. Type `2` to select `Proxy Server`, and then type the name of the proxy server.
6. Type `3` to select `Proxy Server Port`, and then type the proxy server port number.
7. (Optional) You can also specify the proxy server user name (option `4`) and password (option `5`).
8. Type `q` to close scapostinstall.
9. At the command prompt, type `fortifyupdate`.

Related Documents

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

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

All Products

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

Document / File Name	Description
About Fortify Software Documentation About_Fortify_Docs_*<version>*.pdf	This paper provides information about how to access Fortify product documentation. **Note:** This document is included only with the product download.
Fortify Software System	This document provides the details about the

Document / File Name	Description
Requirements Fortify_Sys_Reqs_<*version*>.pdf	environments and products supported for this version of Fortify Software.
Fortify Software Release Notes FortifySW_RN_<*version*>.pdf	This document provides an overview of the changes made to Fortify Software for this release and important information not included elsewhere in the product documentation.
What's New in Fortify Software <version> Fortify_Whats_New_<*version*>.pdf	This document describes the new features in Fortify Software products.

Fortify ScanCentral SAST

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

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

Fortify Software Security Center

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

Document / File Name	Description
OpenText™ Fortify Software Security Center User Guide	This document provides Fortify Software Security Center users with detailed information about how to deploy and use Fortify Software Security Center. It provides all the

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

Fortify Static Code Analyzer

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

Document / File Name	Description
OpenText™ Fortify Static Code Analyzer User Guide SCA_Guide_<*version*>.pdf	This document describes how to install and use Fortify Static Code Analyzer to scan code on many of the major programming platforms. It is intended for people responsible for security audits and secure coding.
OpenText™ Fortify Static Code Analyzer Custom Rules Guide SCA_Cust_Rules_Guide_<*version*>.zip	This document provides the information that you need to create custom rules for Fortify Static Code Analyzer. This guide includes examples that apply rule-writing concepts to real-world security issues. **Note:** This document is included only with the product download.
OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide LIM_Guide_<*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.

Fortify Static Code Analyzer Applications and Tools

The following documents provide information about Fortify Static Code Analyzer applications and tools. These documents are available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-static-code-analyzer-and-tools.

Document / File Name	Description
OpenText™ Fortify Static Code Analyzer Applications and Tools Guide SCA_Apps_Tools_<*version*>.pdf	This document describes how to install Fortify Static Code Analyzer applications and tools. It provides an overview of the applications and command-line tools that enable you to scan your code with Fortify Static Code Analyzer, review analysis results, work with analysis results files, and more.
OpenText™ Fortify Audit Workbench User Guide AWB_Guide_<*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.
OpenText™ Fortify Plugin for Eclipse User Guide Eclipse_Plugin_Guide_<*version*>.pdf	This document provides information about how to install and use the Fortify Plugin for Eclipse to analyze and audit your code.
OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studio User Guide IntelliJ_AnalysisPlugin_Guide_<*version*>.pdf	This document describes how to install and use the Fortify Analysis Plugin for IntelliJ IDEA and Android Studio to analyze your code and optionally upload the results to Fortify Software Security Center.
OpenText™ Fortify Extension for Visual Studio User Guide VS_Ext_Guide_<*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.

About Analyzing the source code

A Fortify Static Code Analyzer security analysis includes the following phases:

- Translate the source code into intermediate files
- Scan the intermediate files to complete the security analysis

There are two ways to analyze your source code:

- Use a locally installed Fortify Static Code Analyzer to perform the entire analysis (translation and scan phases). For information about how to configure and run the analysis locally, see "About scanning locally" on the next page.

  To view the analysis results, upload the analysis results to a Fortify Software Security Center server by doing either of the following:

  - Automatically upload your changes each time you scan your project (see "Integrating with Fortify Software Security Center" below).
  - Manually upload the analysis results (see "Uploading analysis results to Fortify Software Security Center" on page 23).

  Note: You can also open the analysis results (FPR) file in OpenText™ Fortify Audit Workbench.

- Use Fortify ScanCentral SAST to perform the entire analysis (translation and scan phases) or only the scan phase. For information about how to configure and run the analysis using Fortify ScanCentral SAST, see "Scanning with Fortify ScanCentral SAST" on page 24.

  Note: If you use Fortify ScanCentral SAST to perform only the scan phase, then the Fortify Analysis Plugin performs the translation phase using a locally installed Fortify Static Code Analyzer.

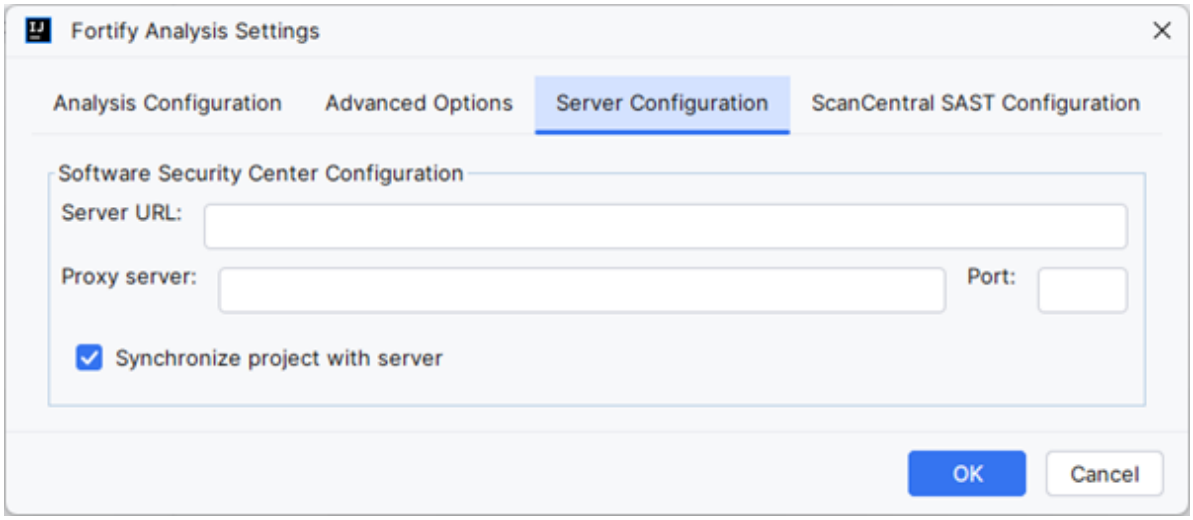
  To view the analysis results, configure the Fortify Analysis Plugin to upload the analysis results to a Fortify Software Security Center server. Alternatively, you can use the provided job token in the Fortify ScanCentral SAST command-line interface to retrieve the analysis results (FPR) file (see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*). You can then open the analysis results file in Fortify Audit Workbench.

Integrating with Fortify Software Security Center

You need to configure a connection to Fortify Software Security Center to upload your analysis results to Fortify Software Security Center whether you analyze your code with a local installation of Fortify Static Code Analyzer or if you use Fortify ScanCentral SAST.

To configure a connection to Fortify Software Security Center:

1. Select **Tools > Fortify > Analysis Settings**.
2. Select the **Server Configuration** tab.



3. In the **Server URL** box, specify the URL for your Fortify Software Security Center server.
4. If required, specify a proxy server and port number.

   Note: If you specify proxy information, exclude the protocol from the proxy server (for example, `some.secureproxy.com`). You must specify a proxy port number for the proxy server.

5. Each time you scan your code locally, the Fortify Analysis Plugin automatically uploads your changes to an application version on Fortify Software Security Center by default. To turn synchronization off, clear the **Synchronize project with server** check box.

   This synchronization helps facilitate collaborative auditing and enables you to synchronize any source code changes each time you rescan the project.

   Note: Automatic synchronization requires that you specify an application version that already exists in Fortify Software Security Center. If the application version does not exist in Fortify Software Security Center, you must first create it. For instructions, see the *OpenText™ Fortify Software Security Center User Guide*.

6. Click **OK**.

See Also

"Uploading analysis results to Fortify Software Security Center" on page 23

About scanning locally

This section describes how to perform a scan of your source code on the local system. In the analysis configuration, you can specify how much memory to use during the scans, the SQL type, select the

security content you want to use, whether you want to scan in quick scan mode, and other advanced scanning options. You can also synchronize the analysis results with Fortify Software Security Center.

OpenText strongly recommends that you periodically update the security content, which contains Secure Coding Rulepacks and external metadata. For information about how to update the security content, see "Updating Fortify Security Content" on page 9.

This section contains the following topics:

About quick scan

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

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

Note: By default, Fortify Software Security Center does not permit you to upload scans performed in quick scan mode. However, you can configure your Fortify Software Security Center application version so that uploaded audit projects scanned in quick scan mode are processed. For more information, see analysis results processing rules in the *OpenText™ Fortify Software Security Center User Guide*.

Configuring local analysis options

Customize the security content and the amount of memory Fortify Static Code Analyzer uses during a local analysis with the analysis settings. You can also specify the SQL type your project uses.

To configure the analysis settings:

1. Select **Tools > Fortify > Analysis Settings**.
   The Fortify Analysis Settings dialog box opens to the **Analysis Configuration** tab.

2. To specify the location of Fortify Static Code Analyzer:
   a. Click **Browse** to the right of **Fortify executable path**.
   b. Go to `<sca_install_dir>/bin/`, and select `sourceanalyzer.exe` (on Windows) or `sourceanalyzer` (on non-Windows).
   c. Click **OK**.
3. To specify the amount of memory to use for the scan, in the **Memory (MB)** box, type an integer.

   Do not allocate more than two thirds of the available physical memory.
4. By default, the Fortify Static Code Analyzer treats SQL files as though they use the T-SQL procedural language on Windows systems and PL/SQL on other platforms. To specify the procedural language for analysis, from the **SQL type** list, select **TSQL** or **PLSQL**.
5. To use specific security content to analyze the project (instead of all the security content):
   a. Under **Security Content**, clear the **Use all installed security content** check box.
   b. In the **Installed Fortify Security Content** list, select the check boxes for the rules to apply during the scan.
   c. If you have custom security content installed, in the **Installed Custom Security Content** list, select the check boxes for the custom security content you want to apply during the scan.
6. Click **OK**.

See Also

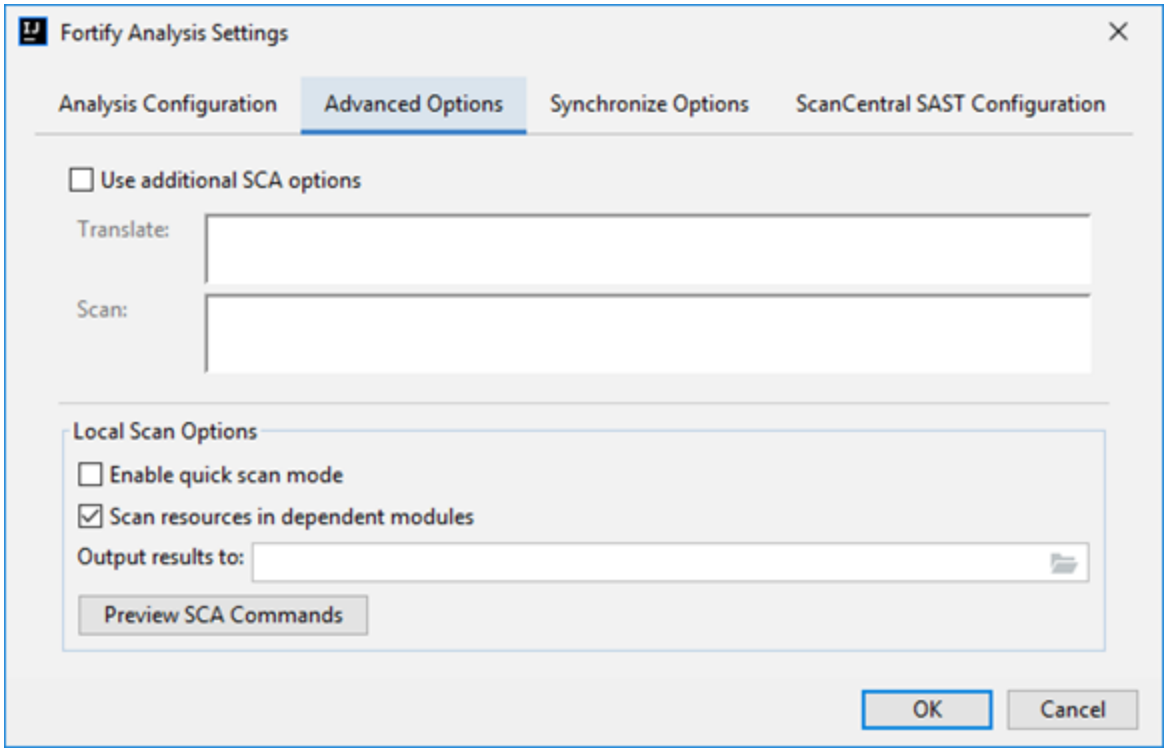
"Configuring advanced local analysis options" below

Configuring advanced local analysis options

Use the advanced analysis settings to customize Fortify Static Code Analyzer translation and scan command-line options. You can also specify whether quick scan mode is enabled, whether to exclude dependent or nested modules, and the location for the analysis results file.

To change the advanced local analysis options:

1. Select **Tools > Fortify > Analysis Settings**.
2. Select the **Advanced Options** tab.



3. Select the **Use additional SCA options** check box.
4. In the **Translate** and **Scan** boxes, type command-line options for the translation and scan phases, respectively.

   For example, if you include the `-verbose` command-line option, the Fortify Analysis Plugin sends detailed status messages to the console during the analysis. For information about the available command-line options, see the *OpenText™ Fortify Static Code Analyzer User Guide*.
5. To change the output location for your analysis results, click **Browse** to the right of the **Output results to** box, and then, in the Select output directory dialog box, specify the directory in which to save the results.

   By default, the analysis results are saved in the source project folder.
6. To enable quick scan, select the **Enable quick scan mode** check box.

   For more information about quick scans, see "About quick scan" on page 16.
7. By default, the Fortify Analysis Plugin includes all source files from dependent modules in scans. To exclude dependent or nested modules from analysis, clear the **Scan resources in dependent modules** check box.

   Although you can scan individual modules, analysis results are more accurate if you scan an entire project together.
8. (Optional) Click **Preview SCA Commands** to see the Fortify Static Code Analyzer command-line options to be used in the analysis.
9. Click **OK**.

See Also

"Configuring local analysis options" on page 16

Scanning projects locally

This topic describes how to use the Fortify Analysis Plugin to analyze your Java source code using the locally installed Fortify Static Code Analyzer to uncover security vulnerabilities.

OpenText strongly recommends that you periodically update the security content, which contains Rulepacks and external metadata. For information about how to update security content, see "Updating Fortify Security Content" on page 9.

Note: If your project is an Android Gradle project, build the release target for the project so that the final project artifacts are generated before the scan. Doing this provides more accurate analysis results. You can either build the release target manually, before you start the scan, or later, as described in the following procedure.

To scan a project on the local system:

1. Do one of the following:
   - Select **Tools > Fortify > Analyze Project**.
   - Right-click a module, and then select **Analyze Module**.

   Note: If your project is an Android Gradle project, the plugin prompts you to build the release target for the project so that the final project artifacts are generated. In the Rebuild the release target dialog box, click **Yes**.
2. If prompted, specify the path to the Fortify Static Code Analyzer executable, and then click **OK**.

   The Fortify Static Code Analyzer scan starts. The progress bar at the bottom of the window displays the progress of events during the scan. After the scan is completed, the Fortify Analysis Plugin saves the resulting Fortify Project Results (FPR) file. By default, the analysis results are saved in the source project folder. You can specify a different output location before you start a scan (see "Configuring advanced local analysis options" on page 17).
3. If the Fortify Analysis Plugin is configured to synchronize with Fortify Software Security Center:
   a. If prompted to login to Fortify Software Security Center:
      i. If you have not already configured the URL for Fortify Software Security Center, type the server URL in the **SSC URL** box.
      ii. From the **Login method** menu, select the login method set up for you on Fortify Software Security Center.
      iii. Depending on the selected login method, follow the procedure described in the following table.

Login Method	Procedure
Username/Password	Type your Fortify Software Security Center user name and password.
Authentication Token	Specify the decoded value of a Fortify Software Security Center authentication token of type ToolsConnectToken. **Note:** For instructions about how to create an authentication token from Fortify Software Security Center, see the *OpenText™ Fortify Software Security Center User Guide*.

b. Select the application version that corresponds to your IntelliJ or Android Studio project, and then click **OK**.

If you have turned off synchronize project with Fortify Software Security Center, you can configure the connection later, and then upload the analysis results (see "Uploading analysis results to Fortify Software Security Center" on page 23).

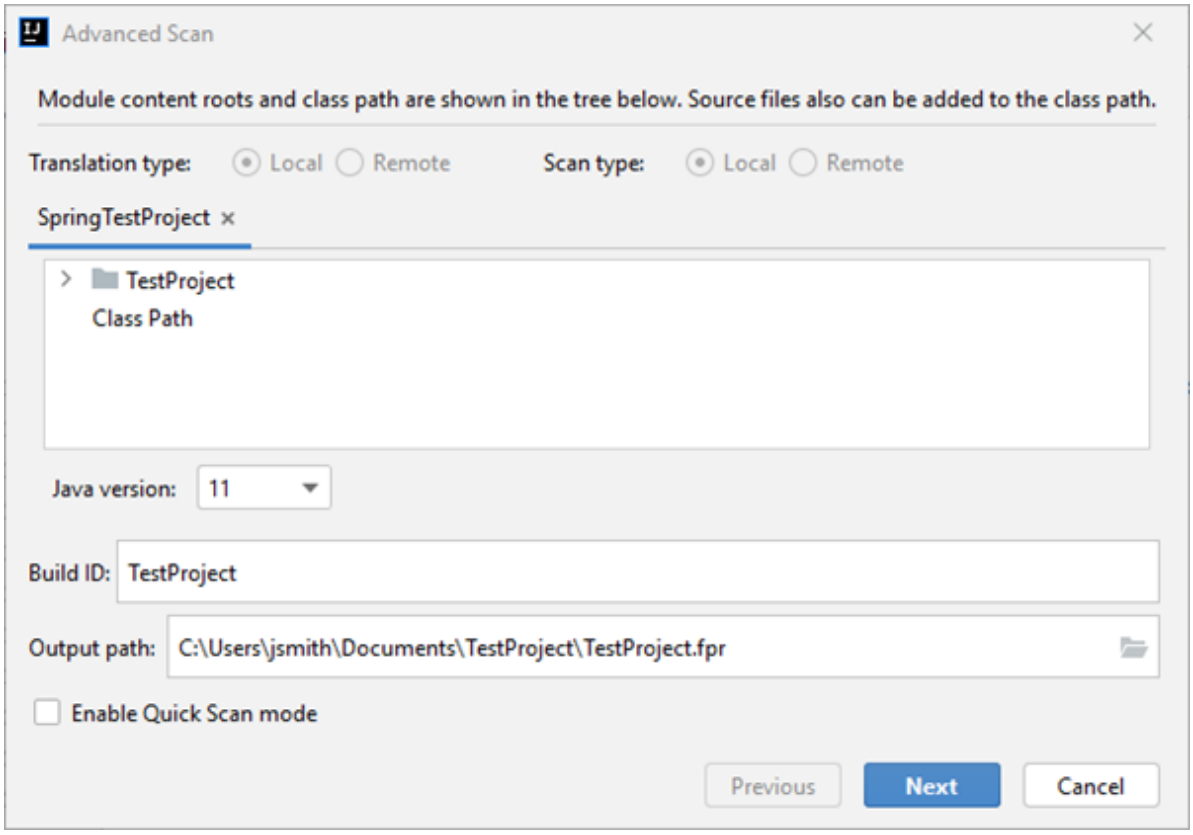
Performing an advanced local scan

Use the advanced scan to change the analysis options from those configured in the analysis settings and perform a local scan for a specific project. Use the advanced scan to translate and analyze Java projects that have source code in multiple directories, have special translation or build conditions, or have files that you want to exclude from the project.

To perform an advanced scan:

1. Select **Tools > Fortify > Advanced Scan**.

   The Advanced Scan wizard automatically includes all source files configured in the IDE.



   If you scan several modules, the wizard displays several tabs, one for each module. All modules are translated separately but analyzed together. If you want to exclude a module, close its tab.

2. Make sure that **Translation type** and **Scan type** are set to **Local**.

   To run an advanced scan with Fortify ScanCentral SAST, see "Performing an advanced scan with Fortify ScanCentral SAST" on page 29.

3. To exclude files or directories that contain, for example, test source code, right-click the file or directory, and then select **Exclude**.
4. The Fortify Analysis Plugin automatically detects the class path from the IntelliJ or Android Studio project settings. To add folders that the plugin has not detected as in the class path, right-click a build directory, and then select **Add to ClassPath**.
5. From the **Java version** list, select the Java version for the project.
6. In the **Build ID** box, type the build ID.

   The project name is the default build ID with unacceptable file system symbols escaped.

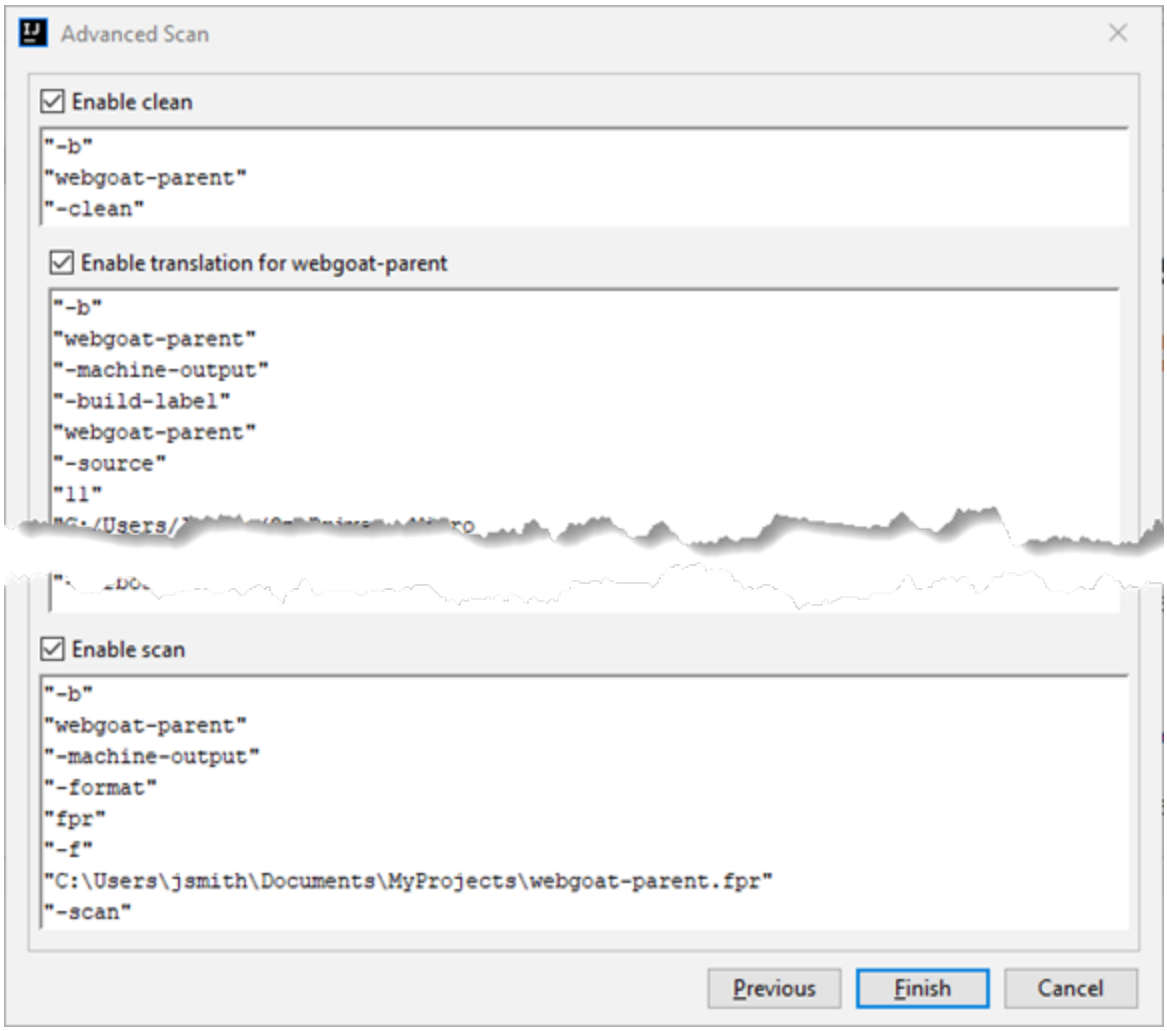
7. To specify a different output file path than the default, in the **Output path** box, type the path and file name for the Fortify Project Results (FPR) file that Fortify Static Code Analyzer will generate.

8. To perform a quick scan, select the **Enable Quick Scan mode** check box.

   For information about quick scans, see "About quick scan" on page 16.

9. Click **Next**.

   A preview of the Fortify Static Code Analyzer command-line options to be used in the analysis is displayed.



   The analysis process includes the following phases:

   - During the *clean* phase, Fortify Static Code Analyzer removes files from a previous translation of the project.
   - During the *translation* phase, you can see one translation section for each of the selected modules. You can modify the class path and all build parameters for each module separately. Fortify Static Code Analyzer translates source code identified in the previous page into an intermediate format associated with the build ID. (The build ID is typically the project name.)
   - During the *scan* phase, Fortify Static Code Analyzer analyzes the source files identified during the translation phase and generates analysis results in the FPR format.

Any additional Fortify Static Code Analyzer options configured on the **Advanced Options** tab in analysis settings are shown here. You can modify any of the Fortify Static Code Analyzer options. For information about the available command-line options, see the *OpenText™ Fortify Static Code Analyzer User Guide*.

10. (Optional) To skip an analysis phase, clear the **Enable clean**, **Enable translation**, or **Enable scan** check box.

    For example, if the security content has changed but the project has not changed, you might want to disable the **translation** phase so that Fortify Static Code Analyzer scans the project without retranslating.
11. Click **Finish**.

Uploading analysis results to Fortify Software Security Center

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

Note: By default, Fortify Software Security Center does not permit you to upload scans performed in quick scan mode. However, you can configure your Fortify Software Security Center application version so that uploaded audit projects scanned in quick scan mode are processed. For more information, see analysis results processing rules in the *OpenText™ Fortify Software Security Center User Guide*.

To upload analysis results to Fortify Software Security Center:

1. Make sure that you have a generated FPR file in the default location (the source project folder) or the location configured in the analysis settings (see "Configuring advanced local analysis options" on page 17).

   The FPR file must already exist.
2. From the IntelliJ or Android Studio menu bar, select **Tools > Fortify > Upload Results to Software Security Center**.

   The Software Security Center Credentials dialog box opens.
3. If prompted to login to Fortify Software Security Center:
   a. If you have not already configured the URL for Fortify Software Security Center, type the server URL in the **SSC URL** box.
   b. From the **Login method** menu, select the login method set up for you on Fortify Software Security Center.
   c. Depending on the selected login method, follow the procedure described in the following table.

Login Method	Procedure
Username/Password	Type your Fortify Software Security Center user name and password.
Authentication Token	Specify the decoded value of a Fortify Software Security Center authentication token of type ToolsConnectToken. **Note:** For instructions about how to create an authentication token from Fortify Software Security Center, see the *OpenText™ Fortify Software Security Center User Guide*.

4. Select the Fortify Software Security Center application version that corresponds to your project, and then click **OK**.

You can now open the application and view the analysis results from Fortify Software Security Center or from the Fortify Remediation Plugin for IntelliJ IDEA and Android Studio. For information about how to view and work with analysis results in Fortify Software Security Center, see the *OpenText™ Fortify Software Security Center User Guide*. For information about how to view and work with analysis results from IntelliJ or Android Studio, see *OpenText™ Fortify Remediation Plugin for IntelliJ IDEA and Android Studio User Guide* in Fortify Remediation Plugin for IntelliJ IDEA and Android Studio Documentation.

Scanning with Fortify ScanCentral SAST

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

With the Fortify Analysis Plugin and Fortify ScanCentral SAST, you can either:

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

  You must translate the project locally if it uses a language that Fortify ScanCentral SAST does not support in remote translation. For a list of supported languages, see the *Fortify Software System Requirements* document.

  You must have a locally installed and licensed Fortify Static Code Analyzer to perform the translation phase.

  Make sure that the Fortify Security Content version on the local system is the same as the version on the Fortify ScanCentral sensor. OpenText strongly recommends that you periodically update the security content. For information about how to update the security content locally, see "Updating Fortify Security Content" on page 9. Use the fortifyupdate utility to update security

content on the Fortify ScanCentral SAST sensor (see the *OpenText™ Fortify Static Code Analyzer User Guide*).

This section contains the following topics:

Requirements to scan with Fortify ScanCentral SAST

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

- A local copy of a Fortify ScanCentral SAST client

  For information on how to obtain a Fortify ScanCentral SAST client, see "Requirements for using the Fortify Analysis Plugin" on page 7.
- A properly configured Fortify ScanCentral SAST installation

  Make sure that the configuration for your Fortify ScanCentral SAST client is authorized with a client authentication token that matches the setting for the Fortify ScanCentral SAST Controller. For more information, see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.
- To connect to Fortify ScanCentral SAST from the Fortify Analysis Plugin, you need either:
  - A ScanCentral SAST Controller URL

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

    - Installed with Fortify Static Code Analyzer: `<sca_install_dir>/jre/lib/security/cacerts/`
    - Installed with Fortify Applications and Tools: `<tools_install_dir>/jre/lib/security/cacerts/`
    - Standalone Fortify ScanCentral SAST client: `<java_home_dir>/lib/security/cacerts`
  - A Fortify Software Security Center URL and an authentication token of type ToolsConnectToken

    To configure the Fortify Software Security Center URL, see "Integrating with Fortify Software Security Center" on page 14.

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

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

  Note: OpenText recommends that the Fortify Software Security Center URL configured in the analysis settings (**Server Configuration** tab) is the same as the Fortify Software Security Center server integrated with the ScanCentral SAST Controller.

- A Fortify Software Security Center authentication token of type ToolsConnectToken

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

See Also

"Requirements for using the Fortify Analysis Plugin" on page 7

Configuring Fortify ScanCentral SAST options

This topic describes how to configure the default Fortify ScanCentral SAST options used when you submit a project for analysis. You can specify how to connect to the Fortify ScanCentral SAST Controller, whether to upload analysis results to Fortify Software Security Center, and other Fortify ScanCentral SAST settings such as inclusion of test files, sensor pool selection, and notification email address). You can also specify Fortify Static Code Analyzer translation and scan options to include in the analysis.

To configure the Fortify ScanCentral SAST options:

1. Select **Tools > Fortify > Analysis Settings**.
2. To configure the Fortify ScanCentral SAST client location:
   a. Select the **Analysis Configuration** tab.
   b. To the right of the **Fortify executable path** box, click the **Browse** button , and do one of the following:
      - If you installed Fortify Static Code Analyzer that includes an embedded Fortify ScanCentral SAST client, go to `<sca_install_dir>/bin/` and select `sourceanalyzer.exe` (on Windows) or `sourceanalyzer` (on non-Windows).
      - To select a standalone client installed with Fortify Applications and Tools, go to `<tools_install_dir>/bin/` and select `scancentral.bat` (on Windows) or `scancentral` (on non-Windows).
      - To select a standalone client installed in a different location, select `scancentral.bat` (on Windows) or `scancentral` (on non-Windows).
3. Select the **ScanCentral SAST Configuration** tab.

4. (Optional) Select **Include test files in scan** to include the test source set (Gradle) or a test scope (Maven) with the scan.
5. To specify how to connect to Fortify ScanCentral SAST, do one of the following:
   - Select **Use Controller URL**, and then in the **Controller URL** box, type the URL for the ScanCentral SAST Controller.

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

     Tip: Click **Test Connection** to confirm that the URL is valid, and the Controller is accessible.
   - Select **Get Controller URL from SSC**, and then in the **Token** box, paste the decoded token value for an authentication token of type ToolsConnectToken.

     Note: For instructions about how to create an authentication token from Fortify Software Security Center, see the *OpenText™ Fortify Software Security Center User Guide*.

     Make sure you that have the Fortify Software Security Center URL that is integrated with the ScanCentral SAST Controller provided on the **Server Configuration** tab (see "Integrating with Fortify Software Security Center" on page 14).

     Tip: Click **Test Connection** to confirm that the URL and token is valid, and the server is accessible.
6. To upload the analysis results to Fortify Software Security Center, do the following:
   a. Select the **Send scan results to SSC** check box.
   b. In the **Token** box, paste the decoded token value for an authentication token of type ToolsConnectToken.

      Note: If you connect to Fortify ScanCentral SAST using a Controller URL, analysis results are uploaded to the Fortify Software Security Center server specifically integrated with the ScanCentral SAST Controller.
7. Under **Sensor pool**, specify whether to use the default sensor pool or to select one from a list of available sensor pools when you run a Fortify ScanCentral SAST scan.

   Note: If Fortify ScanCentral SAST is in SSC lockdown mode, the sensor pool selection is disabled. Fortify ScanCentral SAST automatically uses either the sensor pool associated with a selected application version or the default sensor pool.
8. (Optional) In the **Notification email** box, type an email address for job status notification.

9. (Optional) To specify Fortify Static Code Analyzer command-line options for the translation or scan phase:
   a. Select the **Advanced Options** tab.
   b. Select the **Use additional SCA options** check box and type Fortify Static Code Analyzer command-line options for the translation or scan phase.

      For detailed information about the available Fortify Static Code Analyzer options, see the *OpenText™ Fortify Static Code Analyzer User Guide*.
10. Click **OK** to save the configuration.

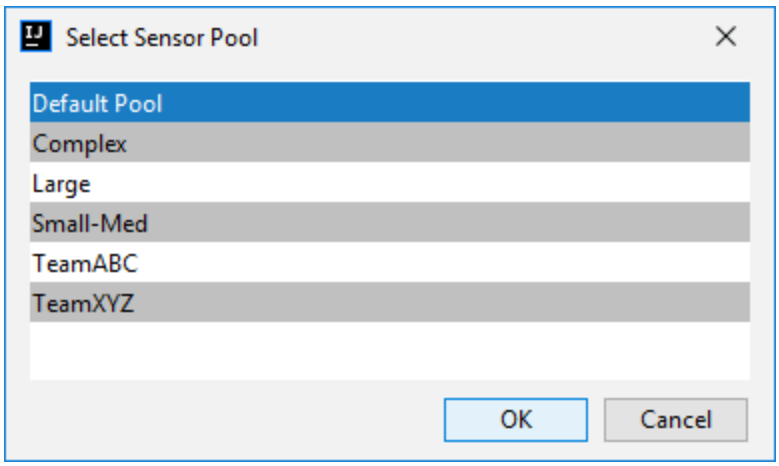
Scanning projects with Fortify ScanCentral SAST

Before you can scan your project with Fortify ScanCentral SAST, you must configure the Fortify ScanCentral SAST options as described in "Configuring Fortify ScanCentral SAST options" on page 26. To override the default Fortify ScanCentral SAST options for a specific project, use the Advanced Scan wizard ("Performing an advanced scan with Fortify ScanCentral SAST" on the next page.

To scan a project with Fortify ScanCentral SAST:

1. Start the scan by doing one of the following:
   - To perform a remote translation and remote scan, select **Tools > Fortify > Analyze Project with ScanCentral > Remote Translation**.
   - To perform a local translation and remote scan, select **Tools > Fortify > Analyze Project with ScanCentral > Local Translation**.
2. If prompted, select the application version where you want to upload the analysis results, and then click **OK**.
3. If prompted, select a sensor pool from the Select Sensor Pool dialog box, and then click **OK**.

   Note: If Fortify ScanCentral SAST is in SSC lockdown mode, then you must select the default sensor pool.



To view the analysis results, you can either:

- Copy the provided job token and use it in the Fortify ScanCentral SAST command-line interface to check the status and retrieve the analysis results (see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*). You can then open the analysis results (FPR) file in Fortify Audit Workbench.

  Tip: If you need to retrieve the job token, you can find it in the Fortify ScanCentral SAST log file. For default log file locations, see "Locating log files" on page 33.

- If you uploaded the analysis results to Fortify Software Security Center, you can check the status of the job (and view the analysis results) on the Fortify Software Security Center server. After the scan is complete, you can use the OpenText™ Fortify Remediation Plugin for IntelliJ IDEA and Android Studio to view the analysis results in IntelliJ or Android Studio (see the *OpenText™ Fortify Remediation Plugin for IntelliJ IDEA and Android Studio User Guide* in Fortify Remediation Plugin for IntelliJ IDEA and Android Studio Documentation).

Performing an advanced scan with Fortify ScanCentral SAST

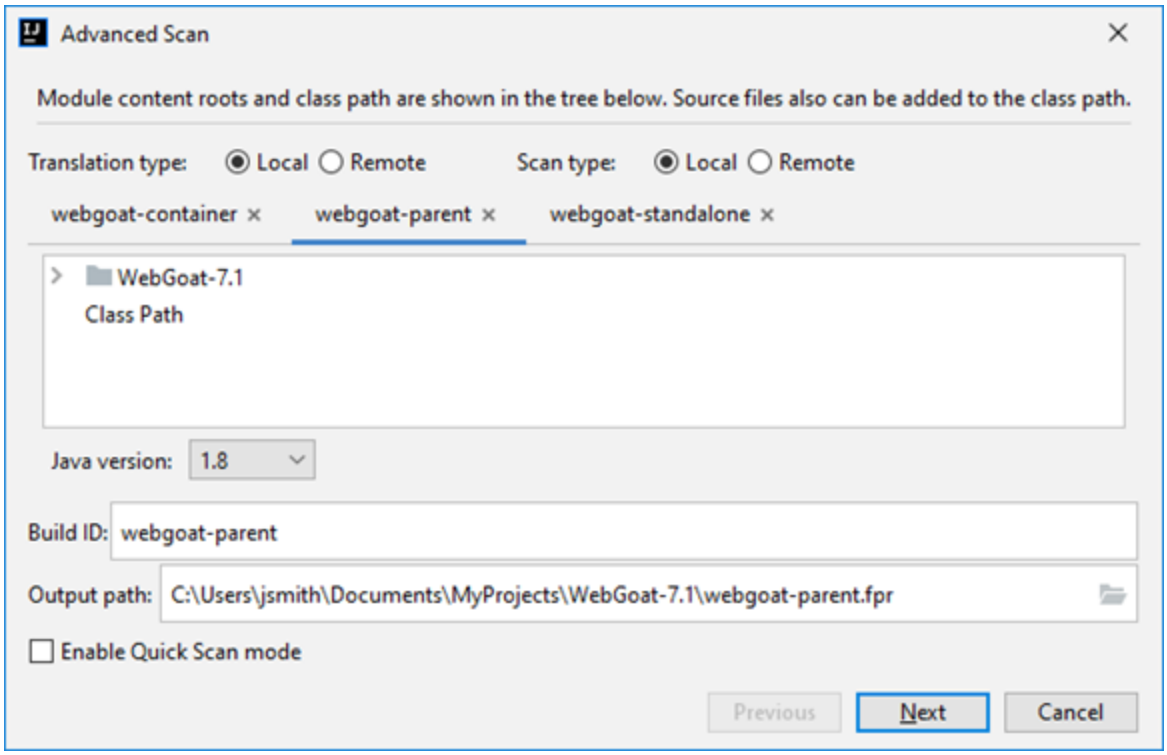
Use the Advanced Scan wizard to change the analysis options for a specific project from those configured in the analysis settings. Make sure that you have a Fortify ScanCentral SAST client configured (see "Requirements to scan with Fortify ScanCentral SAST" on page 25).

Important! To upload the analysis results to Fortify Software Security Center, make sure that you have specified an authentication token in the Fortify ScanCentral SAST configuration. For more information, see "Configuring Fortify ScanCentral SAST options" on page 26.

To perform an advanced scan using Fortify ScanCentral SAST:

1. Select **Tools > Fortify > Advanced Scan**.

   The Advanced Scan wizard automatically includes all source files configured in IntelliJ or Android Studio.



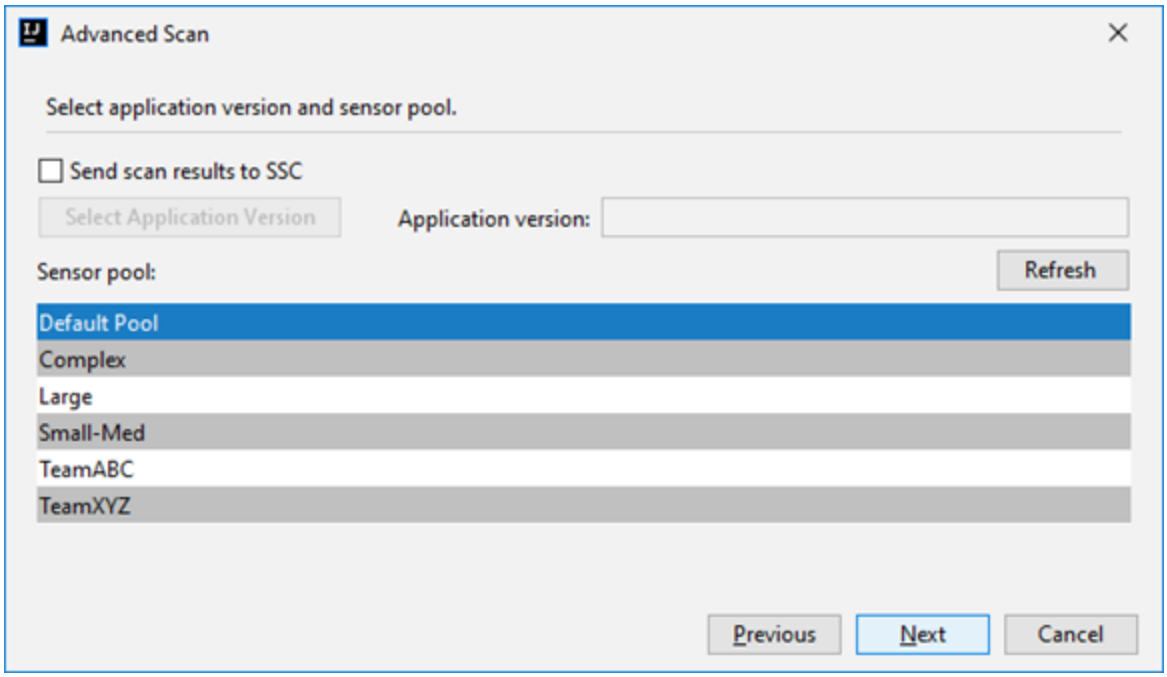
If you scan several modules, the wizard displays a tab for each module. All modules are translated separately but analyzed together. To exclude a module, close its tab.

Note: The following options are only available for analysis performed entirely on a local system: **Java version**, **Build ID**, **Output path**, and **Enable Quick Scan mode**. Ignore these options for analysis with Fortify ScanCentral SAST.

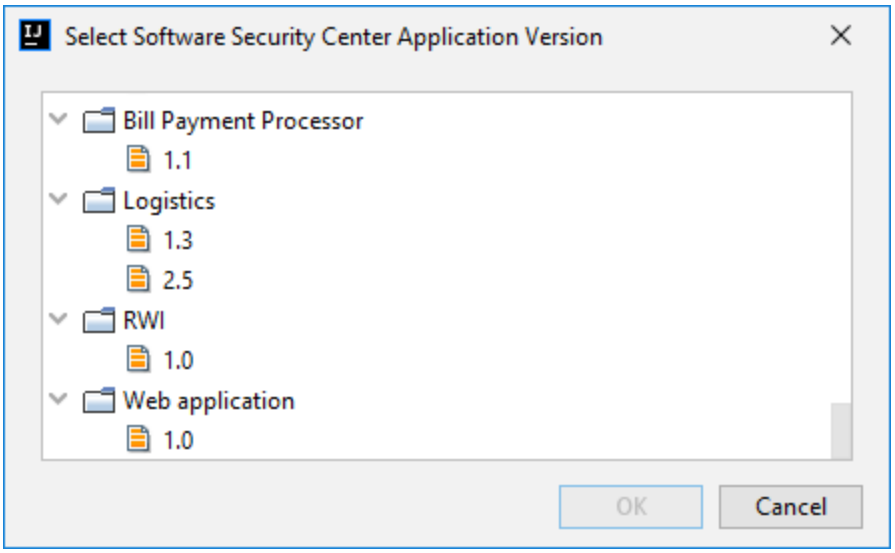
2. Specify where you want to run the translation and scan phases of the analysis by doing one of the following:
   - To run the entire analysis with Fortify ScanCentral SAST, select **Remote** for **Translation type**.

     Note: When you select **Remote** for the translation type, then the Fortify Analysis Plugin automatically sets the **Scan type** to **Remote**.

   - To run the translation phase on the local system and the scan phase with Fortify ScanCentral SAST, select **Local** for **Translation type** and **Remote** for **Scan type**.
   - To run the entire analysis on the local system, select **Local** for both **Translation type** and **Scan type**. Skip the rest of this procedure and see "Performing an advanced local scan" on page 20.
3. To exclude files or directories that contain, for example, test source code, right-click the file or directory, and then select **Exclude**.
4. The Fortify Analysis Plugin automatically detects the class path from the IntelliJ or Android Studio project settings. To add folders that the plugin has not detected in the class path, right-click a build directory and select **Add to ClassPath**.
5. Click **Next**.



6. To upload the analysis results to Fortify Software Security Center, select the **Send scan results to SSC** check box and do the following:
   a. Click **Select Application Version**.

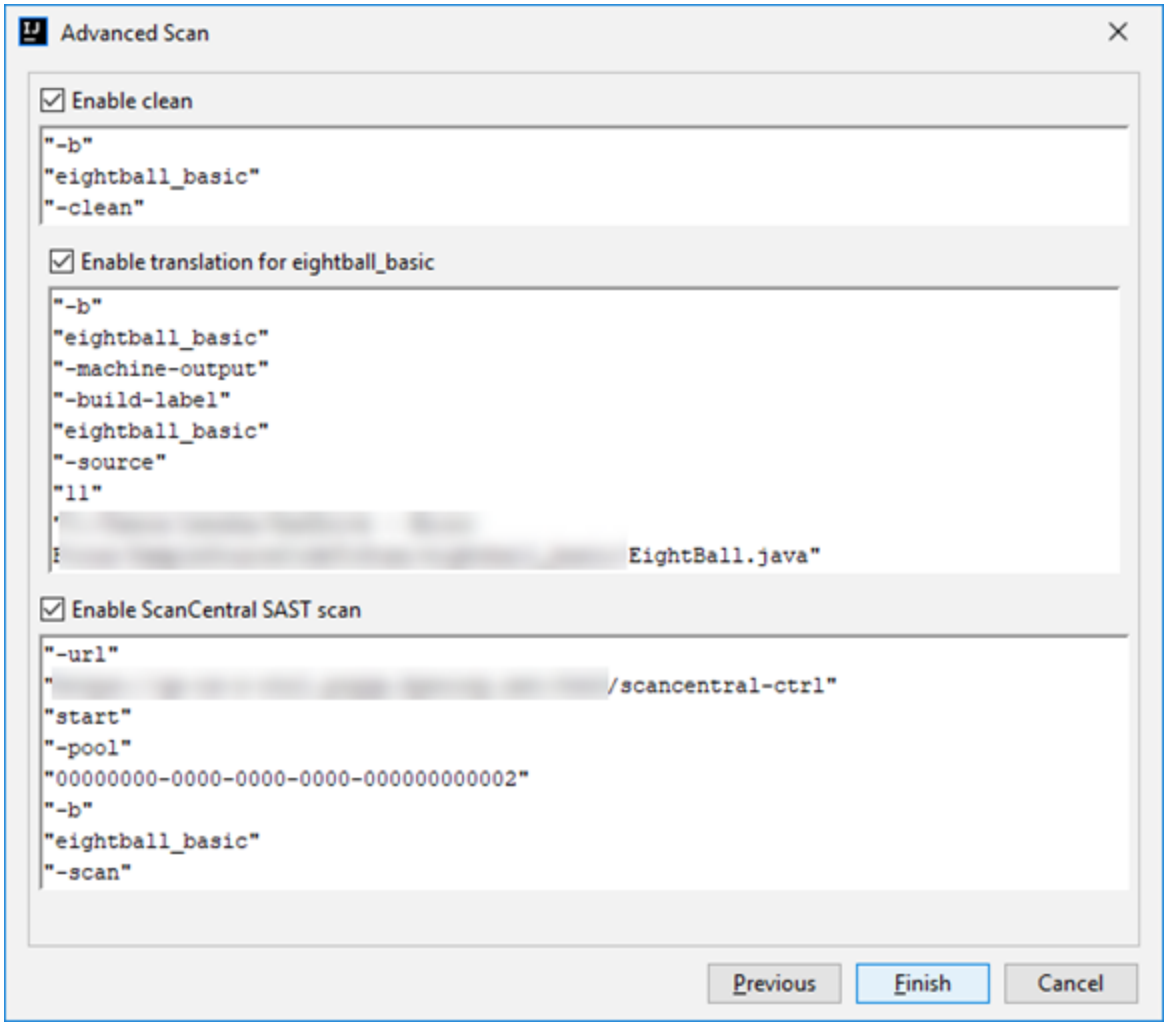


   b. Select the application version where you want to upload the analysis results, and then click **OK**.
7. From the **Sensor pool** list, select a sensor pool.

Note: If Fortify ScanCentral SAST is in SSC lockdown mode, the sensor pool selection is not enabled. Fortify ScanCentral SAST automatically uses either the sensor pool associated with a selected application version or the default sensor pool.

8. Click **Next**.

   A preview of the Fortify Static Code Analyzer and Fortify ScanCentral SAST command-line options for the analysis is displayed. The following image shows an example of a local translation and remote scan preview.



   The preview shows the commands-lines for the following phases:

   - (Local translation only) During the *clean* phase, Fortify Static Code Analyzer removes files from a previous translation of the project.
   - (Local translation only) During the *translation* phase, you can see one translation section for each selected module. You can change the class path and build parameters for each module individually. Fortify Static Code Analyzer translates source code identified in the previous page into an intermediate format associated with the build ID. (The build ID is typically the project name.)

     Any additional Fortify Static Code Analyzer translation options configured on the **Advanced Options** tab in the analysis settings are shown here. You can change any of the Fortify Static Code Analyzer options. For information about the available command-line options, see the *OpenText™ Fortify Static Code Analyzer User Guide*.

- The Fortify Analysis Plugin uses the Fortify ScanCentral SAST start command to start a remote scan. You cannot modify this command.

9. (Optional) To skip an analysis phase, clear the **Enable clean**, or **Enable translation for <proj_name>** check box.
10. Click **Finish**.

Locating log files

For help diagnosing a problem with the Fortify Analysis Plugin, provide the log files to Customer Support. The default locations for the log files are:

- On Windows:
  - C:\Users*<username>*\AppData\Local\Fortify\IntelliJAnalysis-*<version>*\log
  - C:\Users*<username>*\AppData\Local\Fortify\sca*<version>*\log

    Log files in this directory are only created if you analyze the code locally with Fortify Static Code Analyzer.
  - C:\Users*<username>*\AppData\Local\Fortify\scancentral-*<version>*\log

    Log files in this directory are only created if you analyze the code with Fortify ScanCentral SAST.
- On Linux and macOS:
  - *<userhome>*/.fortify/IntelliJAnalysis-*<version>*/log
  - *<userhome>*/.fortify/sca*<version>*/log

    Log files in this directory are only created if you analyze the code locally with Fortify Static Code Analyzer.
  - *<userhome>*/.fortify/scancentral-*<version>*/log

    Log files in this directory are only created if you analyze the code with Fortify ScanCentral SAST.

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 Analysis Plugin for IntelliJ IDEA and Android Studio 24.4.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!