

OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studio

Software Version: 23.2.0

User Guide

Document Release Date: December 2023

Software Release Date: December 2023

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 2015 - 2023 Open Text.

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

Trademark Notices

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

Documentation Updates

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

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

This document was produced on November 03, 2023. 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	5
Contacting Fortify Customer Support	5
For More Information	5
About the Documentation Set	5
Fortify Product Feature Videos	5
Change Log	6
Getting Started	7
About the Fortify Analysis Plugin	7
Requirements for Using the Fortify Analysis Plugin	7
Installing the Fortify Analysis Plugin	8
Fortify Security Content	9
Updating Fortify Security Content	9
Updating Fortify Security Content on a Network that uses a Proxy Server	10
Related Documents	10
All Products	10
Fortify ScanCentral SAST	11
Fortify Software Security Center	11
Fortify Static Code Analyzer	12
Fortify Static Code Analyzer Applications and Tools	13
About Analyzing the Source Code	14
Scanning Locally	14
Setting Memory for Code Analysis	15
Setting the Query Language Type	15
Selecting the Fortify Security Content to Apply During Analysis	16
Using Quick Scan	16
Excluding Dependent Modules from Analysis	17

Specifying Additional Fortify Static Code Analyzer Options	18
Synchronizing with Fortify Software Security Center	19
Scanning Projects Locally	20
Performing an Advanced Local Scan	21
Scanning with Fortify ScanCentral SAST	24
Requirements to Scan with Fortify ScanCentral SAST	25
Configuring Fortify ScanCentral SAST Options	26
Scanning Projects with Fortify ScanCentral SAST	28
Performing an Advanced Scan with Fortify ScanCentral SAST	29
Uploading Analysis Results to Fortify Software Security Center	33
Locating Log Files	34
Send Documentation Feedback	36

Preface

Contacting Fortify Customer Support

Visit the Support website to:

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

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

For More Information

For more information about Fortify software products:

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

About the Documentation Set

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

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

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

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

Fortify Product Feature Videos

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

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

Change Log

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

Software Release / Document Version	Change
23.2.0	Updated: <ul style="list-style-type: none">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: <ul style="list-style-type: none">Changes were made throughout this guide for the introduction of the Fortify Static Code Analyzer Applications and Tools installerBefore 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)
22.2.0	This document contains the Fortify Analysis Plugin content that was previously covered in the <i>Micro Focus Fortify Plugins for JetBrains IDEs and Android Studio User Guide</i> .
22.1.0	Updated: <ul style="list-style-type: none">Minor edits

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 IntelliJ IDEA or Android Studio with OpenText™ Fortify Static Code Analyzer.

This section contains the following topics:

About the Fortify Analysis Plugin	7
Requirements for Using the Fortify Analysis Plugin	7
Installing the Fortify Analysis Plugin	8
Fortify Security Content	9
Related Documents	10

About the Fortify Analysis Plugin

The Fortify Analysis Plugin focuses on scanning your project to identify vulnerabilities quickly and easily 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

To use the Fortify Analysis Plugin, you must have the following:

- A locally installed and licensed Fortify Static Code Analyzer
The Fortify Static Code Analyzer Applications and Tools installer (which includes the Fortify Analysis Plugin) can detect an existing Fortify Static Code Analyzer that is locally installed in the default location or in the same root folder where you installed Fortify Static Code Analyzer applications and tools. If necessary, you are prompted when you first attempt to analyze your code or open the analysis settings to select the location of a locally installed Fortify Static Code Analyzer.
- To analyze your code with Fortify ScanCentral SAST, make sure you select Fortify ScanCentral SAST client as a component during the Fortify Static Code Analyzer installation.

- You must have a properly configured Fortify ScanCentral SAST installation. Make sure the configuration for the Fortify ScanCentral SAST client that you use is properly 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*.
- Local up-to-date Fortify Security Content unless you are using Fortify ScanCentral SAST for remote analysis (see ["Fortify Security Content" on the next page](#))
- 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`.

Installing the Fortify Analysis Plugin

You can install the Fortify Analysis Plugin on Windows, Linux, and macOS. For a list of supported operating system versions, see the [Fortify Software System Requirements](#) document.

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

To install the Fortify Analysis Plugin:

1. Run the Fortify Static Code Analyzer Applications and Tools installation and select the **IntelliJ IDEA Analysis** component from the list of plugins.
2. Start IntelliJ IDEA or Android Studio.
3. Open the Settings dialog box as follows:
 - On Windows or Linux, select **File > Settings**.
 - On macOS, select **<IDE_name> > Preferences**.
4. On the left, select **Plugins**.
5. Select **Install Plugin from Disk**, browse to the `<tools_install_dir>/plugins/IntelliJAnalysis` directory, and then select `Fortify_IntelliJ_Analysis_Plugin_<version>.zip`.
6. Click **OK**.
7. To activate the plugin, restart the IDE.

The menu bar 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)

Fortify provides the ability to write custom rules that add to the functionality of Fortify Static Code Analyzer and the Secure Coding Rulepacks. For example, you might need to enforce proprietary security guidelines or analyze a project that uses third-party libraries or other pre-compiled binaries that are not already covered by the Secure Coding Rulepacks. You can also customize the external metadata to map Fortify issues to different taxonomies, such as internal application security standards or additional compliance obligations. For instructions on how to create your own custom rules or custom external metadata, see the *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](#). Fortify 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 navigate to the `<sca_install_dir>/bin` directory.
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 navigate to the `<scinstall_dir>/bin` directory.
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
<i>About Fortify Software Documentation</i> <code>About_Fortify_Docs_<version>.pdf</code>	This paper provides information about how to access Fortify product documentation. Note: This document is included only with the product download.

Document / File Name	Description
<i>Fortify Software System Requirements</i> Fortify_Sys_Reqs_<version>.pdf	This document provides the details about the environments and products supported for this version of Fortify Software.
<i>Fortify Software Release Notes</i> 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.
<i>What's New in Fortify Software <version></i> 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. 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
<i>OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide</i> 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. 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
<i>OpenText™ Fortify Software Security Center User Guide</i>	This document provides Fortify Software Security Center users with detailed information about how to deploy and use

Document / File Name	Description
SSC_Guide_<version>.pdf	<p>Fortify Software Security Center. It provides all of the information you need to acquire, install, configure, and use Fortify Software Security Center.</p> <p>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 current status of a project.</p>

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
<p><i>OpenText™ Fortify Static Code Analyzer User Guide</i></p> <p>SCA_Guide_<version>.pdf</p>	<p>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.</p>
<p><i>OpenText™ Fortify Static Code Analyzer Applications and Tools Guide</i></p> <p>SCA_Apps_Tools_<version>.pdf</p>	<p>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.</p>
<p><i>OpenText™ Fortify Static Code Analyzer Custom Rules Guide</i></p> <p>SCA_Cust_Rules_Guide_<version>.zip</p>	<p>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.</p> <p>Note: This document is included only with the product download.</p>
<p><i>OpenText™ Fortify License and</i></p>	<p>This document describes how to install, configure, and use</p>

Document / File Name	Description
<i>Infrastructure Manager Installation and Usage Guide</i> LIM_Guide_<version>.pdf	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. 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
<i>OpenText™ Fortify Audit Workbench User Guide</i> 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.
<i>OpenText™ Fortify Plugin for Eclipse User Guide</i> Eclipse_Plugin_Guide_<version>.pdf	This document provides information about how to install and use the Fortify Complete Plugin for Eclipse.
<i>OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studio User Guide</i> IntelliJ_AnalysisPlugin_Guide_<version>.pdf	This document describes how to install and use Fortify Analysis Plugin for IntelliJ IDEA and Android Studio.
<i>OpenText™ Fortify Extension for Visual Studio User Guide</i> 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 and licensed 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 ["Scanning Locally" below](#).

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 ["Synchronizing with Fortify Software Security Center" on page 19](#)).
- Manually upload the analysis results (see ["Uploading Analysis Results to Fortify Software Security Center" on page 33](#)).

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 the 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.

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 configure synchronizing the analysis results with Fortify Software Security Center.

Fortify 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:

Setting Memory for Code Analysis	15
Setting the Query Language Type	15
Selecting the Fortify Security Content to Apply During Analysis	16
Using Quick Scan	16
Excluding Dependent Modules from Analysis	17
Specifying Additional Fortify Static Code Analyzer Options	18
Synchronizing with Fortify Software Security Center	19
Scanning Projects Locally	20
Performing an Advanced Local Scan	21

Setting Memory for Code Analysis

If you plan to analyze large projects, and you want to make sure you do not run out of memory during analysis, consider increasing the amount of memory that Fortify Static Code Analyzer uses for scanning.

To specify the amount of memory that Fortify Static Code Analyzer uses to scan a project:

1. Select **Fortify > Analysis Settings**.

The Fortify Analysis Settings dialog box opens to the **Analysis Configuration** tab.

2. Under **Scan Configuration**, in the **Memory (MB)** box, type an integer.

If no other memory-intensive processes are running, Fortify recommends that you allocate no more than two thirds of the available physical memory.

Note: The Fortify Analysis Plugin warns you if you specify more memory than is physically available to applications on your system.

3. Click **OK**.

Setting the Query Language Type

By default, the Fortify Analysis Plugin treats SQL files as though they use the T-SQL procedural language on Windows systems and PL/SQL on other platforms. (Fortify Static Code Analyzer determines the SQL type setting by the `com.fortify.sca.fileextensions.sql` property in the `fortify-sca.properties` file.)

To set the procedural language for analysis:

1. Select **Fortify > Analysis Settings**.
The Fortify Analysis Settings dialog box opens to the **Analysis Configuration** tab.
2. Under **Scan Configuration**, from the **SQL type** list, select **TSQL** or **PLSQL**.
3. Click **OK**.

Selecting the Fortify Security Content to Apply During Analysis

By default, the Fortify Analysis Plugin uses all available security content to analyze projects. You can narrow the focus of what the Fortify Analysis Plugin looks for during a scan by selecting the security content that it uses to analyze your project.

To specify the security content used to analyze a project:

1. Select **Fortify > Analysis Settings**.
The Fortify Analysis Settings dialog box opens to the **Analysis Configuration** tab.
2. Under **Security Content**, clear the **Use all installed security content** check box.
3. In the **Installed Fortify Security Content** list, select the check boxes for the rules to apply during the scan.
4. 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.
5. Click **OK**.

Using 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. Fortify 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*.

To enable quick scan mode:

1. Select **Fortify > Analysis Settings**.
2. Select the **Advanced Options** tab.
3. Select the **Enable quick scan mode** check box.
4. Click **OK**.

Excluding Dependent Modules from Analysis

By default, the Fortify Analysis Plugin includes all source files from dependent modules in scans. Although you can scan individual modules, analysis results are more accurate if you scan an entire project together.

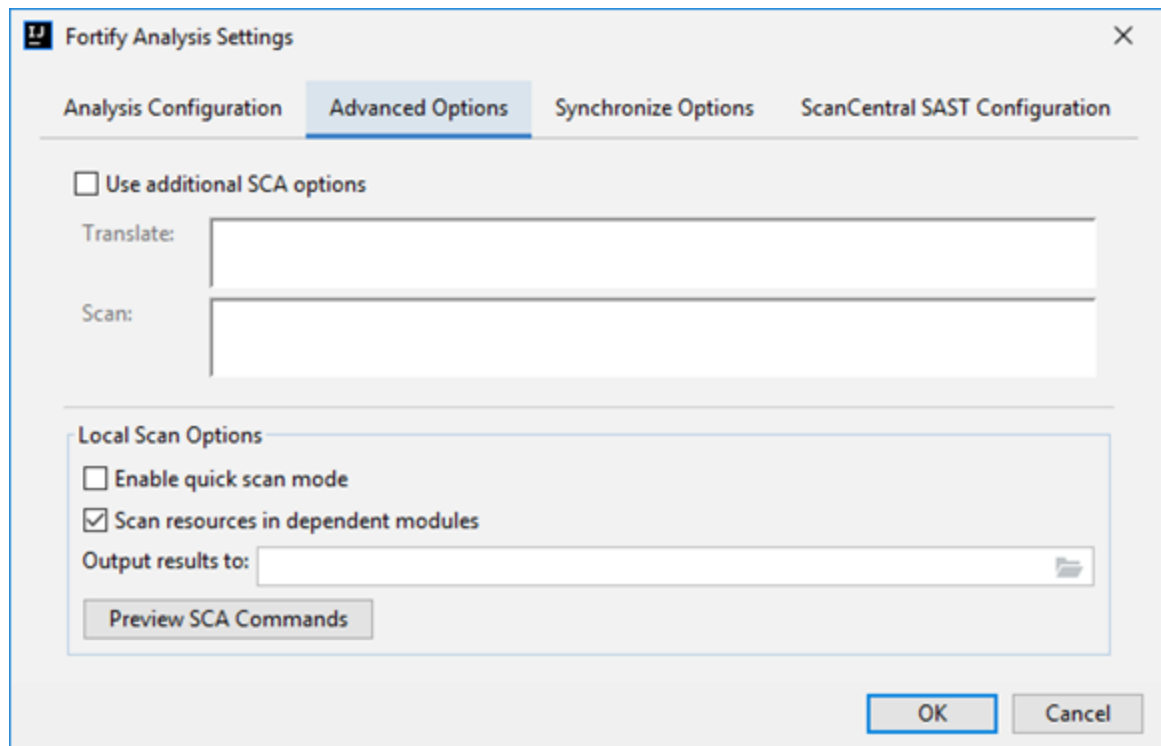
To exclude dependent or nested modules from analysis:

1. Select **Fortify > Analysis Settings**.
2. Select the **Advanced Options** tab.
3. Clear the **Scan resources in dependent modules** check box.
4. Click **OK**.

Specifying Additional Fortify Static Code Analyzer Options

To specify additional Fortify Static Code Analyzer options:

1. Select **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. (Optional) Click **Preview SCA Commands** to see the Fortify Static Code Analyzer command-line options to be used in the analysis.
7. Click **OK**.

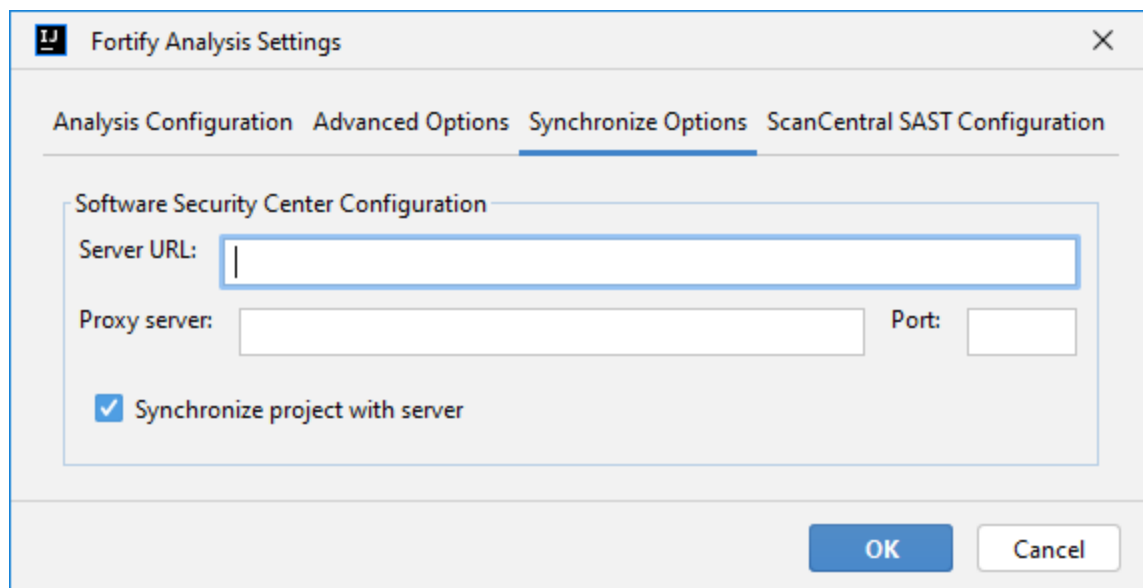
Synchronizing with Fortify Software Security Center

You can automatically upload your changes to an application version on Fortify Software Security Center each time you scan your local project. 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*.

To enable synchronization with Fortify Software Security Center:

1. Select **Fortify > Analysis Settings**.
2. Select the **Synchronize Options** 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: When 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. Select the **Synchronize project with server** check box.
6. Click **OK**.

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.

Fortify 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 **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 prior to a scan (see ["Specifying Additional Fortify Static Code Analyzer Options" on page 18](#)).
3. If your analysis settings are 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.

Login Method	Procedure
Authentication Token	<p data-bbox="722 304 1408 422">Specify the decoded value of a Fortify Software Security Center authentication token of type ToolsConnectToken.</p> <div data-bbox="722 443 1408 636"><p data-bbox="743 451 1386 611">Note: For instructions about how to create an authentication token from Fortify Software Security Center, see the <i>OpenText™ Fortify Software Security Center User Guide</i>.</p></div>

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

If you have disabled 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 33](#)).

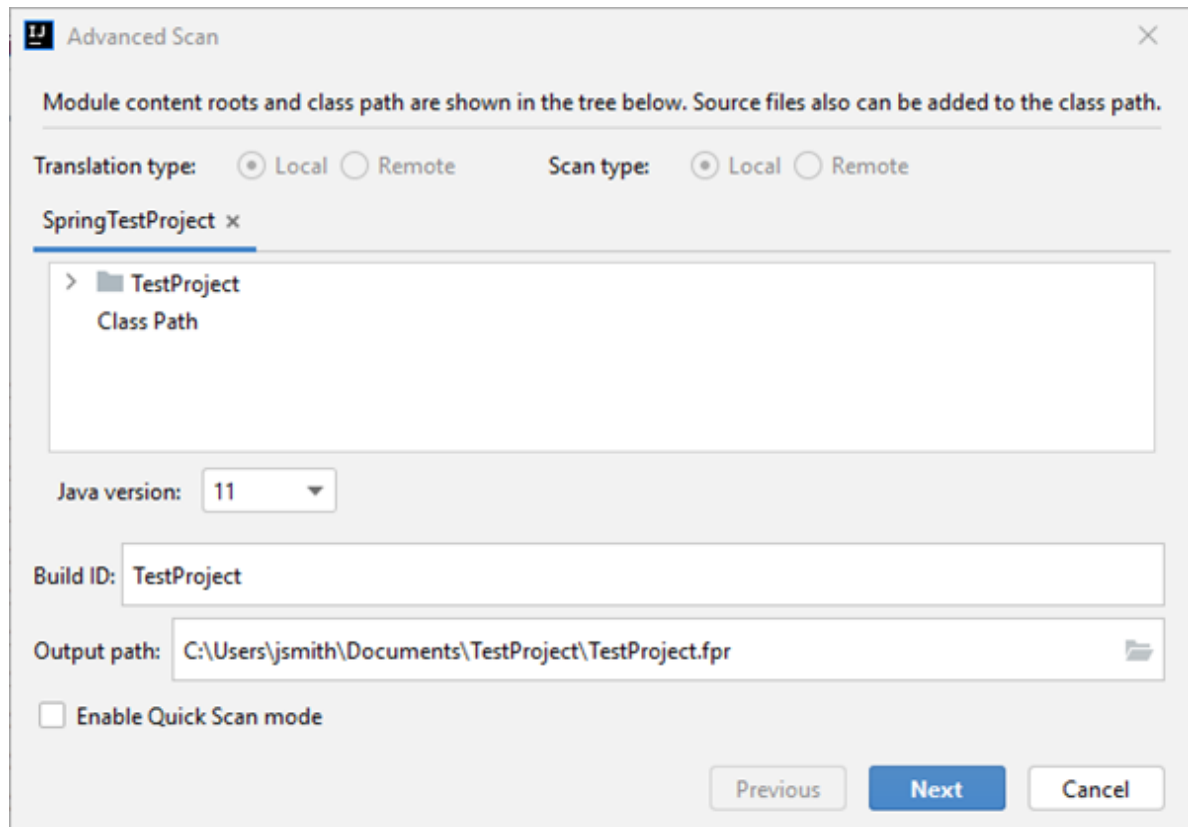
Performing an Advanced Local Scan

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 **Fortify > Advanced Scan**.

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



When 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.

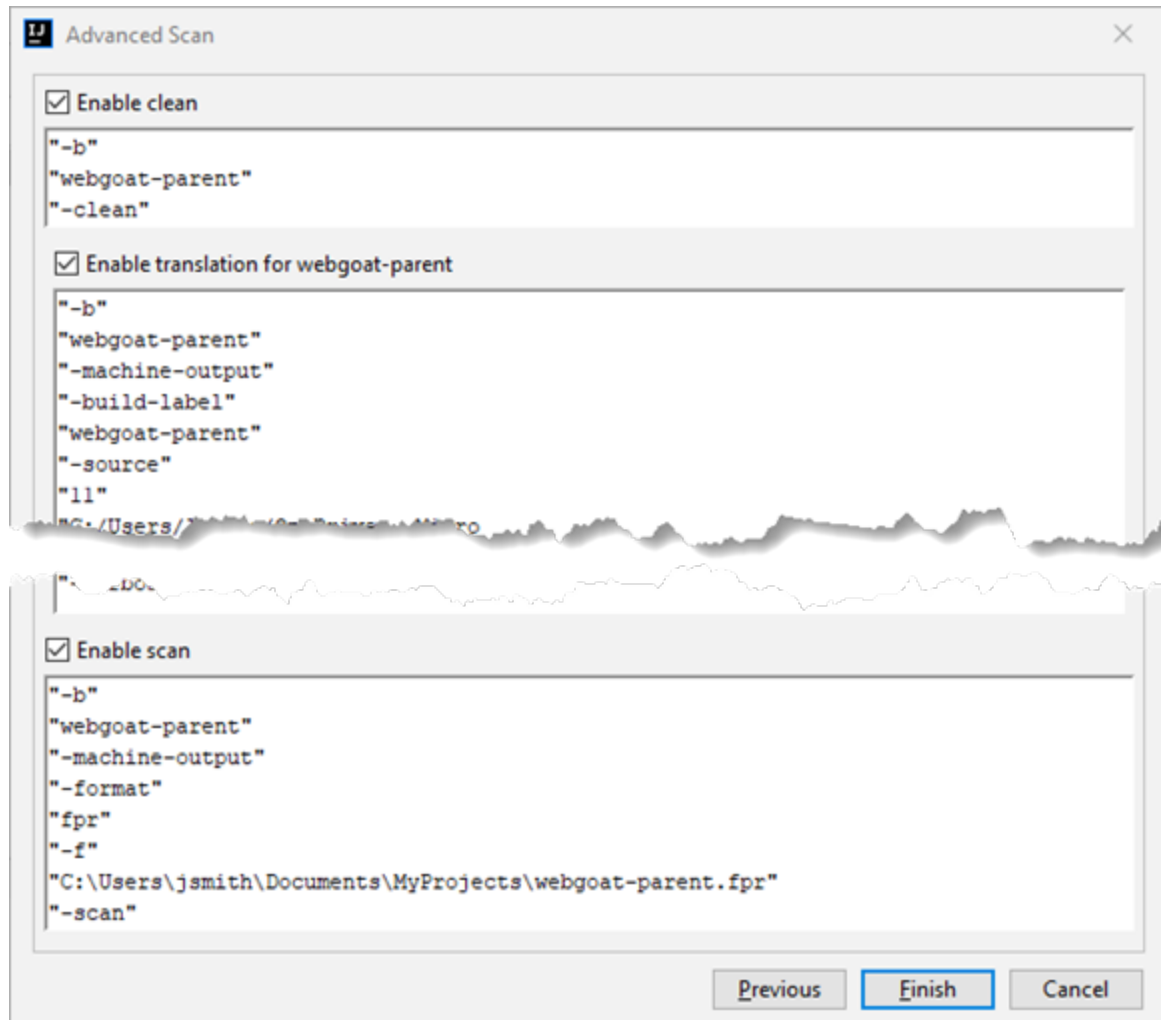
Note: The **Translation type** and **Scan type** options are unavailable when Fortify ScanCentral SAST upload is not enabled. To run an advanced scan with Fortify ScanCentral SAST, see ["Performing an Advanced Scan with Fortify ScanCentral SAST" on page 29](#).

2. To exclude files or directories that contain, for example, test source code, right-click the file or directory, and then select **Exclude**.
3. 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**.
4. From the **Java version** list, select the Java version for the project.
5. In the **Build ID** box, type the build ID.
The project name is the default build ID with unacceptable file system symbols escaped.
6. 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.

- To perform a quick scan, select the **Enable Quick Scan mode** check box.
For information about quick scans, see ["Using Quick Scan" on page 16](#).

- 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 screen 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*.

9. (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.

10. Click **Finish**.

Scanning with Fortify ScanCentral SAST

This section describes the requirements for using Fortify ScanCentral SAST to analyze your code and to upload the analysis results to Fortify Software Security Center. You must provide the Fortify Analysis Plugin with the location of a locally installed Fortify Static Code Analyzer. You are prompted for the location of Fortify Static Code Analyzer the first time you analyze your project or when you open the analysis settings. For instructions about how to configure the Fortify ScanCentral SAST options, see ["Configuring Fortify ScanCentral SAST Options" on page 26](#).

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

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

You must translate the project 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. Fortify 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	25
Configuring Fortify ScanCentral SAST Options	26
Scanning Projects with Fortify ScanCentral SAST	28
Performing an Advanced Scan with Fortify ScanCentral SAST	29

Requirements to Scan with Fortify ScanCentral SAST

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

- A properly configured Fortify ScanCentral SAST installation. Make sure that the configuration for your Fortify ScanCentral SAST client is properly 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 import the certificate into the Java Keystore for Fortify Static Code Analyzer (in `<sca_install_dir>/jre/lib/security`) and for the IDE. For more information, see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

- A Fortify Software Security Center URL and an authentication token of type ToolsConnectToken

To configure the Fortify Software Security Center URL, see ["Synchronizing with Fortify Software Security Center" on page 19](#).

Important! 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 Keystore for Fortify Static Code Analyzer (in `<sca_install_dir>/jre/lib/security`) and for the IDE. For more information, see the *OpenText™ Fortify Software Security Center User Guide*.

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

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

Note: Fortify recommends that the Fortify Software Security Center URL configured in the analysis settings (Synchronize Options) is the same as the Fortify Software Security Center server integrated with the ScanCentral SAST Controller.

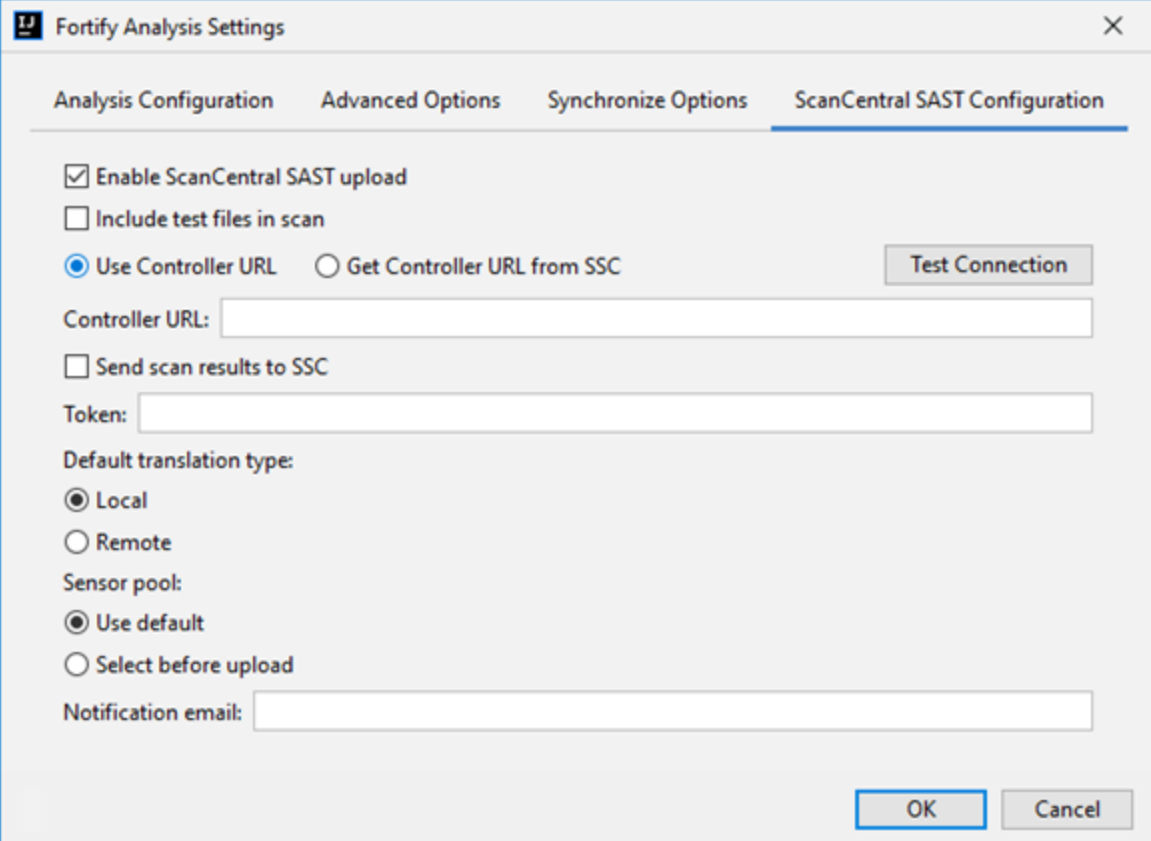
- A Fortify Software Security Center authentication token of type ToolsConnectToken
For instructions about how to create an authentication token, see the *OpenText™ Fortify Software Security Center User Guide*.
- An application version that exists in Fortify Software Security Center
- Permission to access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

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 the translation type (local or remote), the Fortify Static Code Analyzer translation and scan options, the sensor pool selection, and whether to upload analysis results to Fortify Software Security Center.

To configure the Fortify ScanCentral SAST options:

1. Select **Fortify > Analysis Settings**.
2. Select the **ScanCentral SAST Configuration** tab.
3. Select **Enable ScanCentral SAST upload**.



The screenshot shows the 'Fortify Analysis Settings' dialog box with the 'ScanCentral SAST Configuration' tab selected. The dialog has four tabs: 'Analysis Configuration', 'Advanced Options', 'Synchronize Options', and 'ScanCentral SAST Configuration'. The 'ScanCentral SAST Configuration' tab is active and contains the following settings:

- Enable ScanCentral SAST upload
- Include test files in scan
- Use Controller URL Get Controller URL from SSC
- Controller URL:
- Send scan results to SSC
- Token:
- Default translation type:
 - Local
 - Remote
- Sensor pool:
 - Use default
 - Select before upload
- Notification email:

Buttons: 'Test Connection', 'OK', and 'Cancel'.

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 **Synchronize Options** tab (see "[Synchronizing with Fortify Software Security Center](#)" on page 19).

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 **Default translation type**, specify where to run the translation phase of the analysis by selecting one of the following:
 - **Local**—Run the translation phase on the local system and the scan phase with Fortify ScanCentral SAST.
 - **Remote**—Run the entire analysis with Fortify ScanCentral SAST.
8. Under **Sensor pool**, specify whether to use the default sensor pool or to be provided a list of sensor pools to choose from 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.

9. (Optional) In the **Notification email** box, type an email address for job status notification.
10. (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*.

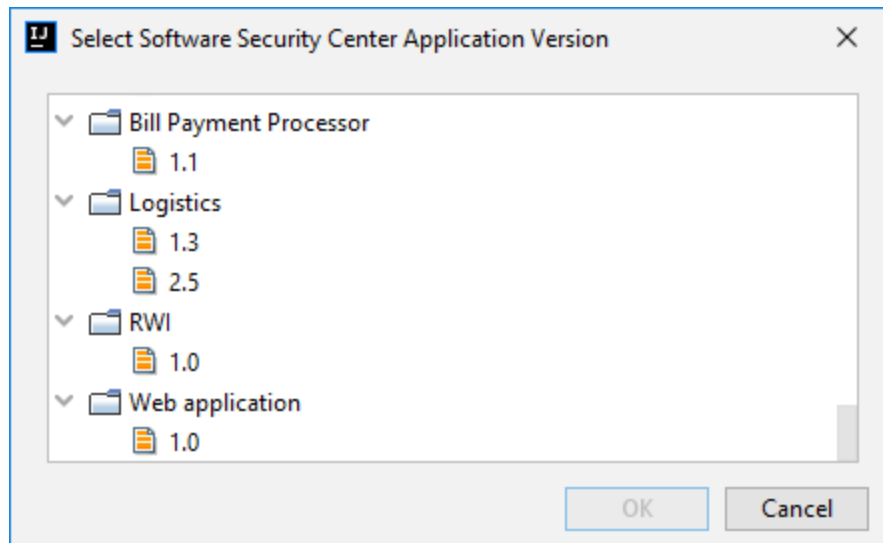
11. Click **OK** to save the configuration.

Scanning Projects with Fortify ScanCentral SAST

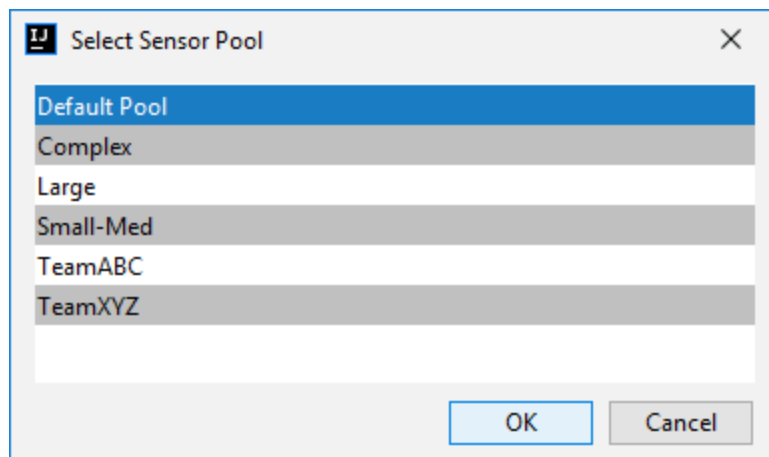
Before you can scan your project with Fortify ScanCentral SAST, you must configure the Fortify ScanCentral SAST options as described in ["Configuring Fortify ScanCentral SAST Options" on page 26](#). If you want to override the default Fortify ScanCentral SAST options for a specific project, use the Advanced Scan wizard (["Performing an Advanced Scan with Fortify ScanCentral SAST" on the next page](#)).

To scan a project with Fortify ScanCentral SAST:

1. Select **Fortify > Analyze Project with ScanCentral**.
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**.



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. The default log file locations are listed in ["Locating Log Files" on page 34](#).

- 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 *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

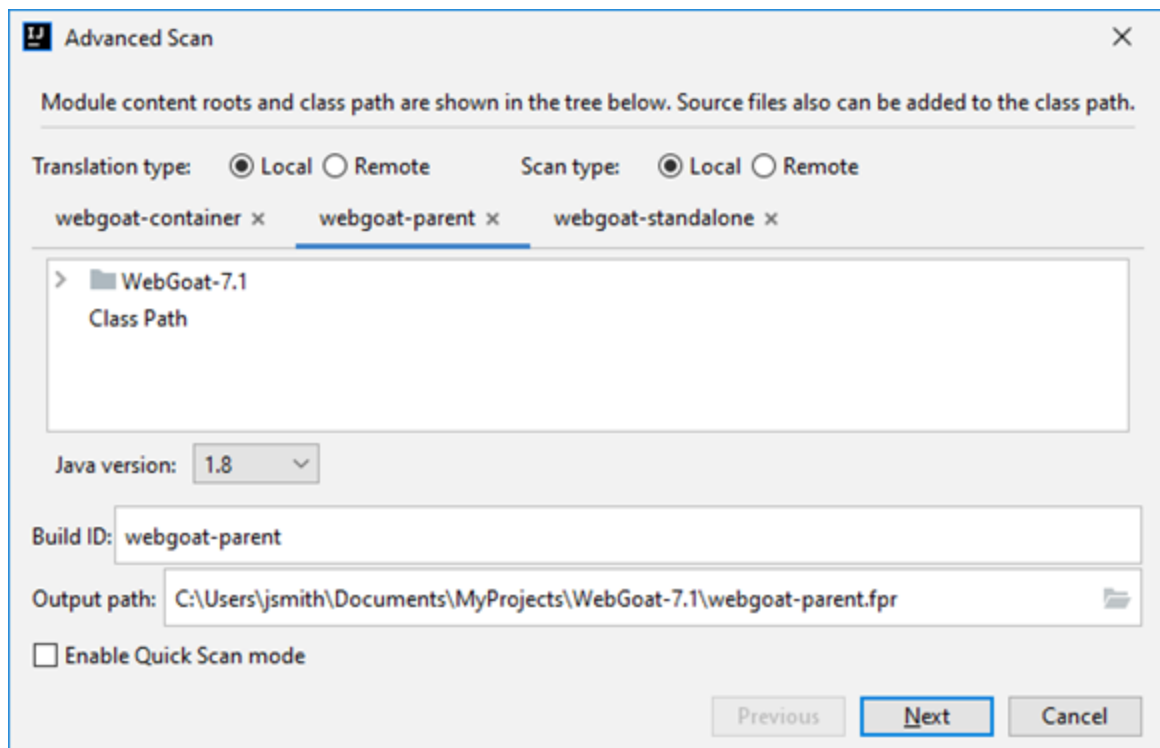
Use the Advanced Scan wizard to change the analysis options for a specific project from those configured in the analysis settings. Make sure that you have enabled Fortify ScanCentral SAST upload (see ["Configuring Fortify ScanCentral SAST Options" on page 26](#)).

Important! If you want 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 **Fortify > Advanced Scan**.

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



When 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**. You can 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 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 with Fortify ScanCentral SAST, select **Remote** for **Translation type**.

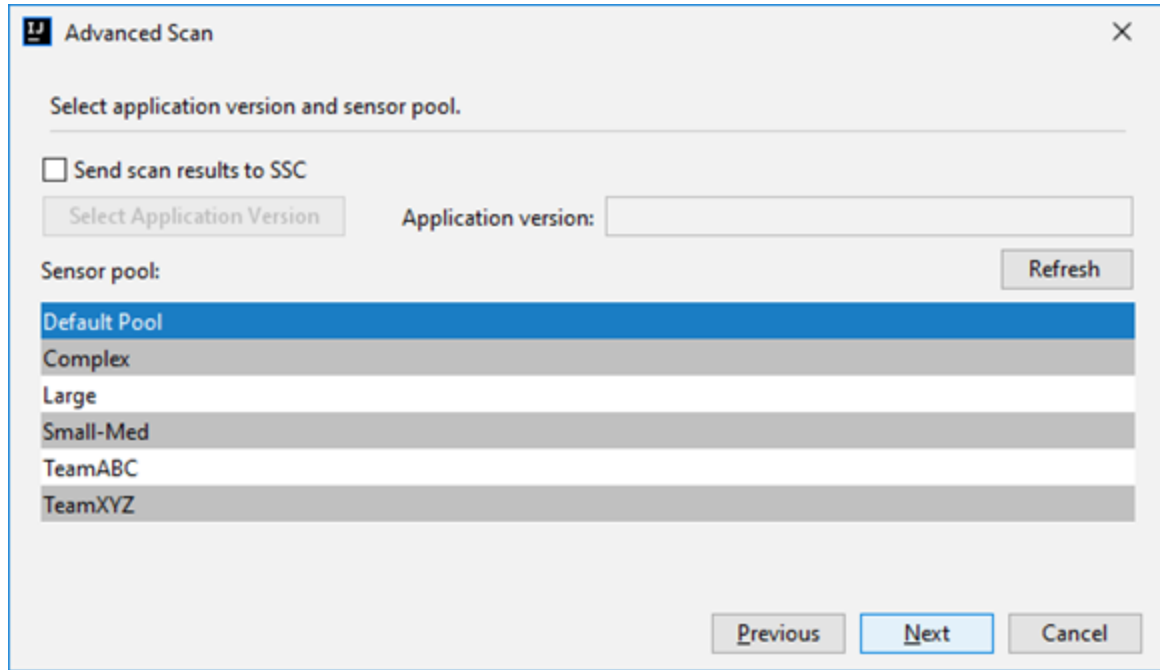
Note: When you select **Remote** for the translation type, then **Scan type** is automatically set to **Remote**.

- 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 21](#).

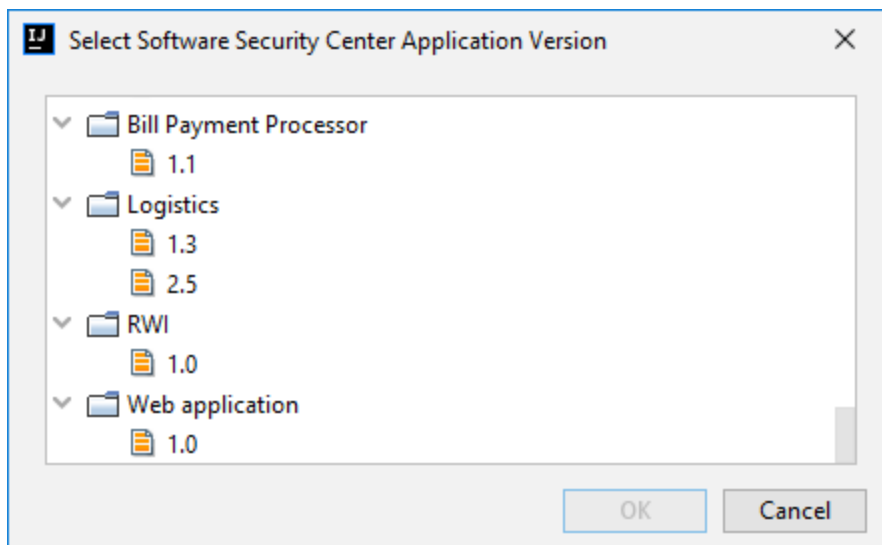
Note: If both the **Translation type** options are disabled and you want to use Fortify ScanCentral SAST for any part of the analysis, you must first enable Fortify ScanCentral SAST upload (see ["Configuring Fortify ScanCentral SAST Options" on page 26](#)).

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**.

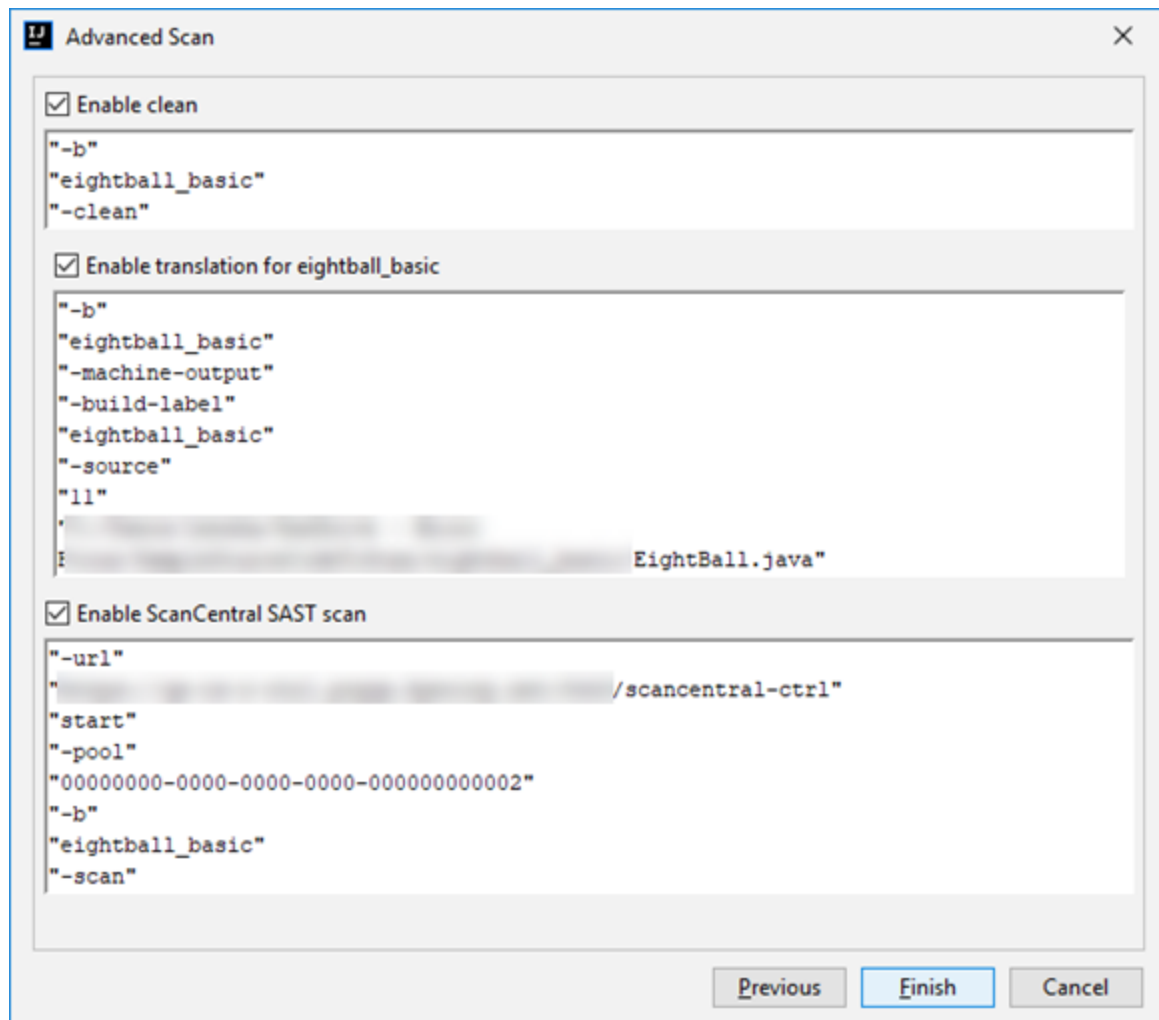
- From the **Sensor pool** list, select a sensor pool.

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.

- Click **Next**.

A preview of the Fortify Static Code Analyzer and Fortify ScanCentral SAST command-line options to be used in 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 modify the class path and build parameters for each module individually. Fortify Static Code Analyzer translates source code identified in the previous screen 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 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*.
 - 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**.

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 step 6 in "[Specifying Additional Fortify Static Code Analyzer Options](#)" on page 18).
The FPR file must already exist.
2. From the IntelliJ or Android Studio menu bar, select **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 <i>OpenText™ Fortify Software Security Center User Guide</i> .

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 *Fortify Remediation Plugin for IntelliJ IDEA and Android Studio User Guide* in [Fortify Remediation Plugin for IntelliJ IDEA and Android Studio Documentation](#).

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 when 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 when 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 when you analyze the code locally with Fortify Static Code Analyzer.
 - `<userhome>/fortify/scancentral-<version>/log`
Log files in this directory are only created when 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 23.2.0)

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!