OpenText™ Fortify Analysis Plugin for IntelliJ IDEA and Android Studio

User Guide

Version 26.4

© Copyright 2026 Open Text

Table of Contents

User Guide 3

1 Change log 3

2 Getting started 3

2.1 Product name changes 4

2.2 About the Fortify Analysis Plugin 4

2.3 Requirements for using the Fortify Analysis Plugin 4

2.4 Installing the Fortify Analysis Plugin 5

2.5 Fortify Security Content 5

2.5.1 Updating Fortify Security Content 5

2.5.2 Updating Fortify Security Content on a network that uses a proxy server 6

2.6 Related Documents 6

3 About Analyzing the source code 8

4 Integrating with Fortify Software Security Center 9

5 About scanning locally 10

5.1 About quick scan 10

5.2 Configuring local analysis options 10

5.3 Configuring advanced local analysis options 11

5.4 Scanning projects locally 11

5.5 Performing an advanced local scan 12

5.6 Uploading analysis results to Fortify Software Security Center 13

6 Scanning with ScanCentral SAST 14

6.1 Requirements to scan with ScanCentral SAST 14

6.2 Configuring ScanCentral SAST options 15

6.3 Scanning projects with ScanCentral SAST 16

6.4 Performing an advanced scan with ScanCentral SAST 17

7 Locating log files 18

User Guide

Software Version: 26.4

Document Release Date: 26.4

Software Release Date: 26.4

1. Change log

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

Software Release / Document Version	Change
26.4.0	Updated: Release date and version number
26.2.0	Updated: Release date and version number
25.4.0	Added: • Added an option to specify the client path when you analyze your code with . (see Configuring ScanCentral SAST options)
25.2.0	Updated: Release date and version number
24.4.0	Updated: • The **Synchronize Options** tab has been renamed **Server Configuration** (see Working with)

2. Getting started

This guide describes how to install the () and use it to scan your code from the IDE with .

This section contains the following topics:

- Product name changes
- About the Fortify Analysis Plugin
- Requirements for using the Fortify Analysis Plugin
- Installing the Fortify Analysis Plugin
- Fortify Security Content
- Related Documents

2.1. Product name changes

is in the process of changing the following product names:

Previous name	New name
Fortify Static Code Analyzer	()
Fortify Software Security Center	OpenText™ Application Security
Fortify WebInspect	()
Fortify on Demand	
Debricked	()
Fortify Applications and Tools	

The product names have changed on product splash pages, mastheads, login pages, and other places where the product is identified. The name changes are intended to clarify product functionality and to better align the Fortify Software products with . In some cases, such as on the documentation title page, the old name might temporarily be included in parenthesis. You can expect to see more changes in future product releases.

2.2. About the Fortify Analysis Plugin

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

After you install the , you can:

- Configure your analysis options and then scan your project locally with or remotely with .
- Upload the to for your organization to manage projects and assign issues to the relevant developers.

2.3. 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 with
  For installation instructions, see the .
- A local client and a properly configured installation
  You can install client, as a component with the installation or from a ZIP archive.

> **Note**
> The ScanCentral SAST client is no longer included in the OpenText SAST installer. The ScanCentral Client needs to be installed separately in order to run SAST as a ScanCentral SAST Sensor.

To upload the to , you need the following:

-
  - The URL
  - A user account with permission to upload to application versions
  - If 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`.

This page is currently under development or is unavailable because it does not exist in the main branch.

About Analyzing the Source Code

2.4. Installing the Fortify Analysis Plugin

You can install the on Windows, Linux, and .

> **Note**
> This page is currently under development or is unavailable because it does not exist in the main branch.

The is available to install from the JetBrains Marketplace or from the IntelliJ IDEA Analysis component installed with .

To install the :

1. Start IntelliJ IDEA or Android Studio.
2. Open the **Settings** or **Preferences**.
3. In the left pane, select **Plugins**.
4. Select the to install by doing one of the following:
    - Install from the JetBrains Marketplace:
        1. Select the **Marketplace** tab, and then in the search box type `Fortify Analysis`.
        2. Select the , and then click **Install**.
    - Install from the installation:
        1. Select **Install Plugin from Disk**.
        2. 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.

2.5. Fortify Security Content

uses a knowledge base of rules to enforce secure coding standards applicable to the codebase for static analysis. consists of and external metadata:

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

provides the ability to write custom rules that add to the functionality of and the . 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 . 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 .

You must have security content on your local system to run a scan locally or to use and run the translation locally (see About Analyzing the Source Code). Typically, you obtain the current when you install . For information about updating Fortify security content, see Updating . strongly recommends that you periodically update the security content.

This section contains the following topics:

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

2.5.1. 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 , type `fortifyupdate`.

If your network uses a proxy server to reach the , see Updating Security Content on a Network That Uses a Proxy Server.

- 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 server. For instructions, see the .

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

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

To specify a proxy for the 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`.

2.6. Related Documents

This topic describes documents that provide information about products.

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_Docs_<*version*>.pdf	This paper provides information about how to access product documentation. **Note** This document is included only with the product download.
Fortify_Sys_Reqs_<*version*>.pdf	This document provides the details about the environments and products supported for this version of Software.
Software Release Notes FortifySW_RN_<*version*>.pdf	This document provides an overview of the changes made to Software for this release and important information not included elsewhere in the product documentation.
What's New in Software <version> Fortify_Whats_New_<*version*>.pdf	This document describes the new features in Software products.
Open Source and Third-Party License Agreements Fortify_OpenSrc_<*version*>.pdf	This document provides open source and third-party software license agreements for software components used in Software.

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

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

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

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

The following documents provide information about . 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
SCA_Guide_<*version*>.pdf	This document describes how to install and use to scan code on many of the major programming platforms. It is intended for people responsible for security audits and secure coding.
SCA_Cust_Rules_Guide_<*version*>.zip	This document provides the information that you need to create custom rules for . This guide includes examples that apply rule-writing concepts to real-world security issues. **Note** This document is included only with the product download.
LIM_Guide_<*version*>.pdf	This page is currently under development or is unavailable because it does not exist in the main branch.

The following documents provide information about 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
SCA_Apps_Tools_<*version*>.pdf	This document describes how to install applications and tools. It provides an overview of the applications and command-line tools that enable you to scan your code with , review analysis results, work with analysis results files, and more.
AWB_Guide_<*version*>.pdf	This document describes how to use to scan software projects and audit analysis results. This guide also includes how to integrate with bug trackers, produce reports, and perform collaborative auditing.
Eclipse_Plugin_Guide_<*version*>.pdf	This document provides information about how to install and use the to analyze and audit your code.
IntelliJ_AnalysisPlugin_Guide_<*version*>.pdf	This document describes how to install and use the to analyze your code and optionally upload the results to .
VS_Ext_Guide_<*version*>.pdf	This document provides information about how to install and use the to analyze, audit, and remediate your code to resolve security-related issues in solutions and projects.

3. About Analyzing the source code

A 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 to perform the entire analysis (translation and scan phases). For information about how to configure and run the analysis locally, see About Scanning Locally.
  To view the , upload the analysis results to a server by doing either of the following:
  - Automatically upload your changes each time you scan your project (see Synchronizing with).
  - Manually upload the (see Uploading Analysis Results to).

  Note
  You can also open the (FPR) file in .

- Use 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 , see Scanning with .

  Note
  If you use to perform only the scan phase, then the performs the translation phase using a locally installed .

  To view the , configure the to upload the to a server. Alternatively, you can use the provided job token in the command-line interface to retrieve the (FPR) file (see the). You can then open the analysis results file in .

4. Integrating with Fortify Software Security Center

You need to configure a connection to to upload your to whether you analyze your code with a local installation of or if you use .

To configure a connection to :

1. Select > **Analysis Settings**.
2. Select the **Server Configuration** tab.
3. In the **Server URL** box, specify the URL for your 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 automatically uploads your changes to an application version on 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 . If the application version does not exist in , you must first create it. For instructions, see the .

6. Click **OK**.

See Also:

Uploading Analysis Results to

5. 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 with .

strongly recommends that you periodically update the security content, which contains and external metadata. For information about how to update the security content, see Updating .

This section contains the following topics:

- About quick scan
- Configuring local analysis options
- Configuring advanced local analysis options
- Scanning projects locally
- Performing an advanced local scan
- Uploading analysis results to Fortify Software Security Center

5.1. About quick scan

Quick scan mode provides a way to quickly scan your projects for critical- and high-priority issues. 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 .

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. 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*.

5.2. 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 > **Analysis Settings**.
   The Fortify Analysis Settings dialog box opens to the **Analysis Configuration** tab.
2. To specify the location of :
   1. Click **Browse** to the right of **Fortify executable path**.
   2. Go to `<sca_install_dir>/bin/` , and select `sourceanalyzer.exe` (on Windows) or `sourceanalyzer` (on non-Windows).
   3. 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 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):
   1. Under **Security Content**, clear the **Use all installed security content** check box.
   2. In the **Installed Fortify Security Content** list, select the check boxes for the rules to apply during the scan.

3. 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**.

This page is currently under development or is unavailable because it does not exist in the main branch.

Configuring Advanced Local Analysis Options

5.3. Configuring advanced local analysis options

Use the advanced analysis settings to customize 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 **> 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 sends detailed status messages to the console during the analysis. For information about the available command-line options, see the .
5. To change the output location for your , 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 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.
7. By default, the 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, are more accurate if you scan an entire project together.
8. (Optional) Click **Preview SCA Commands** to see the command-line options to be used in the analysis.
9. Click **OK**.

See Also:

Configuring Local Analysis Options

5.4. Scanning projects locally

This topic describes how to use the to analyze your Java source code using the locally installed to uncover security vulnerabilities.

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 .



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 . 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 **> 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 executable, and then click **OK**.
   The 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 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).
3. If the is configured to synchronize with :
   1. If prompted to login to Fortify Software Security Center:
      1. If you have not already configured the URL for Fortify Software Security Center, type the server URL in the **SSC URL** box.
      2. From the **Login method** menu, select the login method set up for you on Fortify Software Security Center.
      3. 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*.

   2. 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 , you can configure the connection later, and then upload the (see Uploading Analysis Results to).

5.5. 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 **> 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 , see Performing an Advanced Scan with .

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 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 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.
9. Click **Next**.
   A preview of the command-line options to be used in the analysis is displayed.
   The analysis process includes the following phases:
   - During the *clean* phase, 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. 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, analyzes the source files identified during the translation phase and generates analysis results in the FPR format.

   Any additional options configured on the **Advanced Options** tab in analysis settings are shown here. You can modify any of the options. For information about the available command-line options, see the .
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 scans the project without retranslating.
11. Click **Finish**.

5.6. Uploading analysis results to Fortify Software Security Center

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



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 to :

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).
   The FPR file must already exist.
2. From the IntelliJ or Android Studio menu bar, select **> Upload Results to Software Security Center**.
   The Software Security Center Credentials dialog box opens.
3. If prompted to login to Fortify Software Security Center:
   1. If you have not already configured the URL for Fortify Software Security Center, type the server URL in the **SSC URL** box.
   2. From the **Login method** menu, select the login method set up for you on Fortify Software Security Center.
   3. 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 application version that corresponds to your project, and then click **OK**.

You can now open the application and view the from or from the . For information about how to view and work with in , see the . For information about how to view and work with from IntelliJ or Android Studio, see in Fortify Remediation Plugin for IntelliJ IDEA and Android Studio Documentation.

6. Scanning with ScanCentral SAST

This section describes the requirements, configuration, and procedure to use to analyze your code and upload the to .

With the and , you can either:

- Perform the entire analysis (translation and scan) remotely with
- Perform the translation locally and then automatically upload the translated project to for the scan phase
  You must translate the project locally if it uses a language that does not support in remote translation. For a list of supported languages, see the document.
  You must have a locally installed and licensed to perform the translation phase.
  Make sure that the version on the local system is the same as the version on the Fortify ScanCentral sensor. strongly recommends that you periodically update the security content. For information about how to update the security content locally, see Updating . Use the fortifyupdate utility to update security content on the sensor (see the).

This section contains the following topics:

- Requirements to scan with ScanCentral SAST
- Configuring ScanCentral SAST options
- Scanning projects with ScanCentral SAST
- Performing an advanced scan with ScanCentral SAST

6.1. Requirements to scan with ScanCentral SAST

To analyze your code with , you need the following:

- A local copy of a client
  For information on how to obtain a client, see Requirements for Using the .
- A properly configured installation
  Make sure that the configuration for your client is authorized with a client authentication token that matches the setting for the Controller. For more information, see the .
- To connect to from the , you need either:
  - A 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 client:

- Installed with : `<tools_install_dir>/jre/lib/security/cacerts/`
- Standalone client: `<java_home_dir>/lib/security/cacerts`

- A URL and an authentication token of type ToolsConnectToken
  To configure the URL, see Working with .

To send the to a server, you need the following:

- A URL or a that is integrated with a server.

Note

recommends that the URL configured in the analysis settings (**Server Configuration** tab) is the same as the server integrated with the .

- A authentication token of type ToolsConnectToken
  For instructions about how to create an authentication token, see the .
- An application version that exists in
- Permission to access the application and application version to which you want to upload

This page is currently under development or is unavailable because it does not exist in the main branch.

Requirements for Using the

6.2. Configuring ScanCentral SAST options

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

To configure the options:

1. Select **> Analysis Settings**.
2. For local translation, you must provide the location of a locally installed . If the **Fortify executable path** shows **<Unavailable>**, do the following:
   1. Click **Browse** to the right of **Fortify executable path**.
   2. Go to the installation directory and select the executable file.
      Make sure to set the file type to **sourceanalyzer executable**.
   3. Click **OK**.
3. To configure the client location:
   1. Click **Browse** to the right of **ScanCentral Client Path**
   2. Go to the installation directory and do one of the following:
      - If you are using a standalone client installed with , navigate to `<tools_install_dir> /bin/` and select `scancentral.bat` (on Windows) or `scancentral` (on non-Windows).
      - If the standalone client is installed in a different location, navigate to the installation directory and select `scancentral.bat` (on Windows) or `scancentral` (on non-Windows).
4. Select the **ScanCentral SAST Configuration** tab.
5. (Optional) Select **Include test files in scan** to include the test source set (Gradle) or a test scope (Maven) with the scan.
6. To specify how to connect to , do one of the following:
   - Select **Use Controller URL**, and then in the **Controller URL** box, type the URL for the .

Example
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 , see the .

Make sure you that have the URL that is integrated with the provided on the **Server Configuration** tab (see Working with).

Tip
Click **Test Connection** to confirm that the URL and token is valid, and the server is accessible.

7. To upload the to , do the following:
    1. Select the **Send scan results to SSC** check box.
    2. In the **Token** box, paste the decoded token value for an authentication token of type ToolsConnectToken.

Note
If you connect to using a Controller URL, are uploaded to the server specifically integrated with the .

8. 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 scan.

Note
If is in SSC lockdown mode, the sensor pool selection is disabled. 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 command-line options for the translation or scan phase:
    1. Select the **Advanced Options** tab.
    2. Select the **Use additional SCA options** check box and type command-line options for the translation or scan phase.
    For detailed information about the available options, see the .
11. Click **OK** to save the configuration.

6.3. Scanning projects with ScanCentral SAST

Before you can scan your project with , you must configure the options as described in Configuring Options. To override the default options for a specific project, use the Advanced Scan wizard (Performing an Advanced Scan with .

To scan a project with :

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**.
- If prompted, select the application version where you want to upload the , and then click **OK**.
- If prompted, select a sensor pool from the Select Sensor Pool dialog box, and then click **OK**.

> **Note**
> If is in SSC lockdown mode, then you must select the default sensor pool.

To view the , you can either:

- Copy the provided job token and use it in the command-line interface to check the status and retrieve the (see the). You can then open the (FPR) file in .

> **Tip**
> If you need to retrieve the job token, you can find it in the log file. For default log file locations, see Locating Log Files.

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

6.4. Performing an advanced scan with 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 client configured (see Requirements to Scan with).

> **Important**
> To upload the to , make sure that you have specified an authentication token in the configuration. For more information, see Configuring ScanCentral SAST options.

To perform an advanced scan using :

1. Select **> 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 .

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 , select **Remote** for **Translation type**.

     > **Note**
     > When you select **Remote** for the translation type, then the automatically sets the **Scan type** to **Remote**.

   - To run the translation phase on the local system and the scan phase with , 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.

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 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 to , select the **Send scan results to SSC** check box and do the following:
    1. Click **Select Application Version**.
    2. Select the application version where you want to upload the , and then click **OK**.
7. From the **Sensor pool** list, select a sensor pool.

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

8. Click **Next**.
   A preview of the and 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, 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. 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 translation options configured on the **Advanced Options** tab in the analysis settings are shown here. You can change any of the options. For information about the available command-line options, see the .
    - The uses the 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**.

7. Locating log files

For help diagnosing a problem with the , provide the log files to . 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 .
    - C:\Users\<*username*>\AppData\Local\Fortify\scancentral-<*version*>\log
      Log files in this directory are only created if you analyze the code with .
- On Linux and :
    - <*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 .
    - <*userhome*>/.fortify/scancentral-<*version*>/log
      Log files in this directory are only created if you analyze the code with .

© Copyright 2026 Open Text

For more info, visit https://docs.microfocus.com