
Micro Focus Fortify Jenkins Plugin

Software Version: 19.2.0

User Guide

Document Release Date: November 2019

Software Release Date: November 2019



Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

<https://www.microfocus.com>

Warranty

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

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2014 - 2019 Micro Focus or one of its affiliates

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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 07, 2019. 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-and-services/documentation>

Contents

| | |
|--|----|
| Preface | 5 |
| Contacting Micro Focus Fortify Customer Support | 5 |
| For More Information | 5 |
| About the Documentation Set | 5 |
| Change Log | 6 |
| Chapter 1: Introduction | 7 |
| Software Requirements | 8 |
| What's New in this Release | 9 |
| Related Documents | 10 |
| Micro Focus Fortify CloudScan | 10 |
| Micro Focus Fortify Software Security Center | 10 |
| Micro Focus Fortify Static Code Analyzer | 11 |
| Chapter 2: Installation and Configuration | 12 |
| Installing the Fortify Jenkins Plugin | 12 |
| Verifying the Fortify Jenkins Plugin Installation | 12 |
| Preparing Fortify Software Security Center to Work with the Fortify Jenkins Plugin | 13 |
| Configuring Global Settings for the Fortify Jenkins Plugin | 14 |
| Chapter 3: Using the Fortify Jenkins Plugin | 17 |
| Configuring Fortify Analysis with Freestyle Projects | 17 |
| Creating a Post-Build Action to Translate and Scan Remotely | 17 |
| Creating a Post-Build Action to Translate Locally and Scan Remotely | 19 |
| Creating a Post-Build Action to Translate and Scan Locally | 22 |
| Configuring Fortify Analysis with Pipeline Jobs | 27 |
| Pipeline Steps to Translate and Scan Remotely | 27 |
| fortifyRemoteArguments Step | 29 |
| fortifyRemoteArguments Example | 29 |
| fortifyRemoteAnalysis Step | 29 |

| | |
|---|----|
| fortifyRemoteAnalysis Example | 31 |
| Pipeline Steps to Translate locally and Scan Remotely | 32 |
| fortifyRemoteScan Step | 33 |
| fortifyRemoteScan Example | 34 |
| Pipeline Steps to Translate and Scan Locally | 35 |
| fortifyUpdate Step | 38 |
| fortifyUpdate Example | 38 |
| fortifyClean Step | 38 |
| fortifyClean Example | 39 |
| fortifyTranslate Step | 39 |
| fortifyTranslate Examples | 42 |
| fortifyScan Step | 44 |
| fortifyScan Example | 45 |
| fortifyUpload Step | 46 |
| fortifyUpload Example | 47 |
| Viewing Analysis Results | 47 |
| Security Vulnerability Graph for Your Project | 48 |
| Viewing Issues | 49 |
| Configuring the Number of Issues Displayed on a Page | 50 |
| Send Documentation Feedback | 51 |

Preface

Contacting Micro Focus Fortify Customer Support

If you have questions or comments about using this product, contact Micro Focus Fortify Customer Support using one of the following options.

To Manage Your Support Cases, Acquire Licenses, and Manage Your Account

<https://softwaresupport.softwaregrp.com>

To Call Support

1.844.260.7219

For More Information

For more information about Fortify software products:

<https://software.microfocus.com/solutions/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 Micro Focus Product Documentation website:

<https://www.microfocus.com/support-and-services/documentation>

Change Log

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

| Software Release / Document Version | Changes |
|--|---|
| 19.2.0 | Updated: <ul style="list-style-type: none">• Changes were made throughout this document to describe the new ability to perform a Fortify Static Code Analyzer analysis on a remote system using Fortify CloudScan. |
| 19.1.0 | Added: <ul style="list-style-type: none">• "Configuring Fortify Analysis with Pipeline Jobs" on page 27 Updated: <ul style="list-style-type: none">• "Installing the Fortify Jenkins Plugin" on page 12 - Instructions now describe how to obtain the plugin from the Jenkins website• "Creating a Post-Build Action to Translate and Scan Locally" on page 22<ul style="list-style-type: none">• New field added to specify source files for .NET type projects, the upload wait time setting was changed to polling interval, and other minor changes• Changes were made to the description of how to configure uploading results to Fortify Software Security Center |
| 18.20 | Updated to describe the new capability that enables you to scan projects with Fortify Static Code Analyzer as part of the build. |

Chapter 1: Introduction

Use the Fortify Jenkins Plugin in your continuous integration builds to identify security issues in your source code with Micro Focus Fortify Static Code Analyzer. A Fortify Static Code Analyzer security analysis consists of the following phases:

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

The Fortify Jenkins Plugin provides three ways to analyze your source code:

- Offload the complete analysis (translation and scan) to Fortify CloudScan
See "[Software Requirements](#)" on the next page for a list of languages that this method of analysis supports.
- Perform a translation on the local system and then offload the more CPU-intensive scan phase to Fortify CloudScan
- Perform the complete analysis (translation and scan) on the local system

You can run the analysis locally with Gradle, Maven, MSBuild, and Visual Studio (devenv). You can also analyze your source code without a build tool.

After the Fortify Static Code Analyzer analysis is complete, you can upload the analysis results to a Fortify Software Security Center server.

For complete analysis run locally only: If you upload the analysis results to a Micro Focus Fortify Software Security Center server, you can view the analysis result details within Jenkins. The results provide metrics for each build and an overview of the results, without requiring you to log into Fortify Software Security Center.

This content provides instructions for how to install, configure, and use the plugin.

Software Requirements

The Fortify Jenkins Plugin works with the software packages listed in the following table. Your specific requirements depend on the build tools you are using. This table also provides information to help you prepare to add Fortify Static Code Analyzer analysis to your jobs.

| Software | Version | Notes |
|---|-----------------|--|
| Micro Focus Fortify Static Code Analyzer | 18.20 or later | <p>To scan your project locally with Fortify Static Code Analyzer, you must either have the path to the Fortify Static Code Analyzer installation directory so you can specify it in the configuration or make sure that the PATH environment variable includes the sourceanalyzer executable (see "Configuring Global Settings for the Fortify Jenkins Plugin" on page 14).</p> <p>Note: Performing remote analysis requires Fortify Static Code Analyzer version 19.2.0 or later.</p> |
| Micro Focus Fortify Software Security Center (Optional) | 18.20 or later | <p>To upload scan results to Fortify Software Security Center, to trigger a build failure based on scan results, and to see results in Jenkins, make sure that you have:</p> <ul style="list-style-type: none">• The Fortify Software Security Center URL• A Fortify Software Security Center authentication token of type CIToken (see "Preparing Fortify Software Security Center to Work with the Fortify Jenkins Plugin" on page 13) <p>To perform a remote analysis, make sure that you have:</p> <ul style="list-style-type: none">• A Fortify Software Security Center authentication of type CloudCtrlToken (see "Preparing Fortify Software Security Center to Work with the Fortify Jenkins Plugin" on page 13) |
| Micro Focus Fortify CloudScan (Optional) | 19.2.0 or later | <p>To perform a Fortify Static Code Analyzer analysis on a remote system using Fortify CloudScan, make sure that you have the CloudScan Controller URL.</p> <p>Note: If you plan to upload remote scan results to Fortify Software Security Center, then you do not need to provide a CloudScan Controller URL. The Fortify Jenkins Plugin automatically determines the CloudScan Controller that is associated with Fortify Software Security Center.</p> |

| Software | Version | Notes |
|------------------------|-----------------------|--|
| | | <p>Fortify CloudScan supports offloading project translation for .NET (.NET Core, .NET Standard, C#, VB.NET), ABAP, Apex, Classic ASP, ColdFusion, Java (including Gradle and Maven projects), JavaScript, PHP, PL/SQL, Python, Ruby, T-SQL, TypeScript, and Visual Basic.</p> <p>Note: Translation of .NET requires .NET Framework version 4.6.1 or later.</p> |
| Maven | 3.x | <p>To integrate the scan with Maven, you must install the Fortify Maven plugin, which is available when you install Fortify SCA and Apps. Fortify recommends that you use the same Fortify Maven Plugin version as the Fortify Static Code Analyzer version and that you install the source version of the Fortify Maven Plugin rather than the binary version.</p> <p>You must install the Fortify Maven Plugin for the same user who is running Jenkins.</p> <p>If you use a proxy, then you need to configure proxy settings for the Fortify Maven Plugin. For information, see the Settings Reference at https://maven.apache.org.</p> <p>For more information about build integration with the Fortify Maven Plugin, see the <i>Micro Focus Fortify Static Code Analyzer User Guide</i>.</p> |
| MSBuild | 4.x, 12.0, 14.0, 15.0 | |
| Visual Studio (devenv) | 2013, 2015, 2017 | |

What's New in this Release

With this release, you no longer must install and run Fortify Static Code Analyzer on the Jenkins server for projects in most languages. You can now offload the Fortify Static Code Analyzer translation and/or scan to a remote system using Micro Focus Fortify CloudScan. This new capability is available in both Freestyle and Pipeline projects.

Related Documents

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

Note: You can find the Micro Focus Fortify Product Documentation at <https://www.microfocus.com/support-and-services/documentation>.

Micro Focus Fortify CloudScan

The following document provides information about Fortify CloudScan. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website at <https://www.microfocus.com/documentation/fortify-software-security-center>.

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

Micro Focus Fortify Software Security Center

The following documents provide information about Fortify Software Security Center. Unless otherwise noted, these documents are available on the Micro Focus Product Documentation website at <https://www.microfocus.com/documentation/fortify-software-security-center>.

| Document / File Name | Description |
|---|---|
| <i>Micro Focus Fortify Software Security Center User Guide</i> SSC_Guide_<version>.pdf | <p>This document provides Fortify Software Security Center users with detailed information about how to deploy and use Software Security Center. It provides all of the information you need to acquire, install, configure, and use 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</p> |

| Document / File Name | Description |
|----------------------|--|
| | developers. Software Security Center provides security team leads with a high-level overview of the history and current status of a project. |

Micro Focus Fortify Static Code Analyzer

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

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

Chapter 2: Installation and Configuration

This section describes how to install the Fortify Jenkins Plugin and how to configure and use the plugin.

This section contains the following topics:

| | |
|--|----|
| Installing the Fortify Jenkins Plugin | 12 |
| Preparing Fortify Software Security Center to Work with the Fortify Jenkins Plugin | 13 |
| Configuring Global Settings for the Fortify Jenkins Plugin | 14 |

Installing the Fortify Jenkins Plugin

To install the Fortify Jenkins Plugin, you must have Jenkins installed on your system. See the *Micro Focus Fortify Software System Requirements* document for the supported Jenkins versions.

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 Jenkins Plugin:

1. From Jenkins, select **Manage Jenkins > Manage Plugins**.
2. On the **Plugin Manager** page, click the **Available** tab.
3. In the **Filter** box, type Fortify.
4. Select the checkbox for the **Fortify** plugin, and then click either **Install without restart** or **Download and install after restart**.

For more information about how to install Jenkins plugins, see the Jenkins website.

Verifying the Fortify Jenkins Plugin Installation

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 verify that the Fortify Jenkins Plugin is installed:

1. Open a browser window and navigate to the Jenkins server URL.
By default, the Jenkins URL is `http://localhost:8080`.
2. From the Jenkins menu, select **Manage Jenkins > Manage Plugins**.
3. On the **Plugin Manager** page, click the **Installed** tab.
4. Verify that **Fortify Jenkins Plugin** is included in the list of installed plugins.

Preparing Fortify Software Security Center to Work with the Fortify Jenkins Plugin

To perform the following tasks, you need to obtain an authentication token created in Fortify Software Security Center. You will use this authentication token to configure the Fortify Jenkins Plugin to communicate with Fortify Software Security Center or Fortify CloudScan. The following table describes the tasks and the token type needed to perform the task.

| Task | Token Type |
|--|---|
| Upload local Fortify Static Code Analyzer scan results to Fortify Software Security Center | CIToken Note: Do not use the JenkinsToken type as it will be removed in a future release. |
| Perform a remote Fortify Static Code Analyzer analysis using Fortify CloudScan (this includes the ability to upload the remote scan results to Fortify Software Security Center) | CloudCtrlToken |

You can generate the authentication token from either the Administration view in Fortify Software Security Center or from the command-line with the `fortifyclient` utility.

Note: If you generate the token from Fortify Software Security Center, use the decoded token to configure the Fortify Jenkins Plugin.

The following instructions describe how to create the authentication token with the `fortifyclient` utility. For information about how to create an authentication token from Fortify Software Security Center, see the *Micro Focus Fortify Software Security Center User Guide*.

To create an authentication token using the `fortifyclient` utility:

1. From the `<ssc_install_dir>/Tools/fortifyclient/bin` directory, run the following:

```
fortifyclient token -gettoken <token_type> -url <ssc_url> -user <user_name> [-daysToLive <number_of_days>]
```

Note: Find the `Tools` folder in the directory where the Fortify Software Security Center WAR file was extracted.

where:

- `<token_type>` is either `CIToken` to upload locally-created FPR files to Fortify Software Security Center or `CloudCtrlToken` for offloading the analysis to a remote system.
- `<ssc_url>` includes both the port number and the context path `/ssc`. For example, `http://my.domain.com:8080/ssc`.
- `<user_name>` is the Fortify Software Security Center username of an account that has the required privileges to read or write information from or to Fortify Software Security Center.
- `<number_of_days>` is the number of days before the token expires. The default is 365.

You are prompted for a password.

2. Type the password for `<user_name>`.

The `fortifyclient` utility displays a token of the general form:

```
cb79c492-0a78-44e3-b26c-65c14df52e86.
```

3. Copy the returned token to use when you configure the Fortify Jenkins Plugin (see "[Configuring Global Settings for the Fortify Jenkins Plugin](#)" below).

Configuring Global Settings for the Fortify Jenkins Plugin

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 configure your Jenkins server so that it can analyze your project and upload results to Fortify Software Security Center using the Fortify Jenkins Plugin:

1. Open a browser window and navigate to the Jenkins server URL.
2. From the Jenkins menu, select **Jenkins > Manage Jenkins > Configure System**.
3. To analyze (translate or scan) your project locally with Fortify Static Code Analyzer, create a Jenkins environment variable to specify the location of the Fortify Static Code Analyzer executables. In **Global properties**, create the following environment variable:
 - **Name:** `FORTIFY_HOME`
 - **Value:** `<sca_install_dir>`
where `<sca_install_dir>` is the path where Fortify Static Code Analyzer is installed. For example, the default location on Windows is `C:\Program Files\Fortify\Fortify_SCA_and_Apps_19.2.0`.

- To upload results from a local analysis to Fortify Software Security Center, scroll down to the **Fortify Assessment** section, and then do the following in the **Software Security Center configuration** section:

Fortify Assessment

Software Security Center configuration

SSC URL

⚠ URL cannot be empty

Authentication token

⚠ Authentication token cannot be empty

Use proxy

Issue template ▼



Maximum issues per page

- In the **SSC URL** box, type the Fortify Software Security Center server URL.
The correct format for the Fortify Software Security Center URL is:
`<protocol>://<ssc_host>:<port>/ssc` (for example:
`http://my.domain.com:8080/ssc`).
- In the **Authentication token** box, type the authentication token of type CIToken generated for the Fortify Software Security Center server.
See "[Preparing Fortify Software Security Center to Work with the Fortify Jenkins Plugin](#)" on page 13.
- To connect to Fortify Software Security Center with a proxy server, select **Use proxy**, and then specify the proxy information.
- From the **Issue template** list, select the appropriate issue template for your projects.
Fortify Software Security Center uses the selected issue template when it creates new applications. The issue template optimizes the categorization, summary, and reporting of the application version data.
- To test the connection to Fortify Software Security Center, click **Test SSC connection**.
- To specify the maximum number of issues to display per page in the results breakdown table, type a number in the **Maximum issues per page** box.

Note: You are not required to specify a value in the **Maximum issues per page** box at this time. You can change this setting later. This setting controls the **Issue Breakdown** table view. The default is 50 issues per page.

- To perform a Fortify Static Code Analyzer analysis on a remote system, do the following in the **Controller configuration** section:

Controller configuration

| | |
|------------------|---|
| Controller URL | <input type="text"/> |
| |  Controller URL cannot be empty |
| Controller token | <input type="text"/> |
| |  Controller token cannot be empty |
| | <input type="button" value="Test Controller connection"/> |

- In the **Controller URL** box, type the CloudScan Controller URL.

Note: If you specify a URL in the **Software Security Center configuration** section (**SSC URL**), then the Fortify Jenkins Plugin automatically determines the CloudScan Controller URL from Fortify Software Security Center and you do not need to provide a CloudScan Controller URL.

The correct format for the CloudScan Controller URL is:

`<protocol>://<controller_host>:<port>/cloud-ctrl` (for example:
`https://myControllerHost.com:8443/cloud-ctrl`).

- In the **Controller token** box, type the Controller authentication token of type CloudCtrlToken.
See "[Preparing Fortify Software Security Center to Work with the Fortify Jenkins Plugin](#)" on [page 13](#) for instructions.
- Click **Save**.

Chapter 3: Using the Fortify Jenkins Plugin

This section describes how to add Fortify analysis to a project as a post-build action or with a Pipeline script.

This section contains the following topics:

- [Configuring Fortify Analysis with Freestyle Projects](#) 17
- [Configuring Fortify Analysis with Pipeline Jobs](#) 27
- [Viewing Analysis Results](#) 47

Configuring Fortify Analysis with Freestyle Projects

The Fortify Jenkins Plugin supports Freestyle and Multi-configuration projects. This section describes how to add Fortify analysis as a post-build action for your job.

Note: The Fortify Jenkins Plugin also supports Jenkins Pipeline. For instructions, see "[Configuring Fortify Analysis with Pipeline Jobs](#)" on page 27.

Creating a Post-Build Action to Translate and Scan Remotely

To configure a post-build action to perform a complete analysis on a remote system:

1. From Jenkins, select an existing job to view or create a new job.
If you selected an existing job, click **Configure** on the job page.
2. In the **Post-build Actions** section, click **Add post-build action**, and then select **Fortify Assessment**.
3. Select **Remote translation & remote scan**.
4. From the **Application type** list, select the type of project you want to analyze. The following table provides instructions for each application type.

| Application Type | Description |
|------------------|--|
| Gradle | <ol style="list-style-type: none">a. To include the test source set (for Java projects only) with translation, select the Include tests check box.b. In the Build file box, type the name of the build file if it is different than the default of <code>build.gradle</code>. |

| Application Type | Description |
|------------------|--|
| Maven | <ul style="list-style-type: none"> a. To include a test scope (for Java projects only) with translation, select the Include tests check box. b. In the Build file box, type the name of the build file if it is different than the default of <code>pom.xml</code>. |
| PHP | <ul style="list-style-type: none"> a. In the PHP version box, type the PHP version used in the project. |
| Python | <ul style="list-style-type: none"> a. In the Python version box, select the Python version used in the project. The default version is 2. b. In the Python virtual environment box, type the location (directory) of the Python virtual environment. c. In the Python requirements file box, type the name of the Python project requirements file used to install and collect dependencies. |
| Other | Use this option to translate and scan other languages. See "Software Requirements" on page 8 for the list of languages that Fortify CloudScan supports for remote translation and scan. |

5. (Optional) To specify Fortify Static Code Analyzer translation options, click **Advanced**, and then specify translation options.

For descriptions of the available translation options, see the *Micro Focus Fortify Static Code Analyzer User Guide*.

Note: Enclose each option and parameter in double quotes. For example, this option excludes test files from the translation: `"-exclude" "C:/ProjA/tests/*"`.

6. (Optional) To specify CloudScan Controller settings, add Fortify Static Code Analyzer scan options, custom Rulepacks, or a scan filter file, click **Optional configuration**. The following table describes the optional configuration settings.

| Field | Description |
|--------------------|--|
| Sensor pool | Specify a sensor pool UUID defined in Fortify Software Security Center. By default, Fortify CloudScan uses the default sensor pool as defined in Fortify Software Security Center. |
| Notification email | Specify the email address to which the Controller will send notifications. |

| Field | Description |
|------------------------------|--|
| Fortify SCA scan options | Specify Fortify Static Code Analyzer scan options. For descriptions of the available scan options, see the <i>Micro Focus Fortify Static Code Analyzer User Guide</i> . Note: Enclose each option and parameter in double quotes. In the following example, two analyzers and quick scan mode are enabled for the scan: <code>"-analyzers" "controlflow,dataflow" "-quick"</code> . |
| Custom Rulepacks | Specify custom rules files (*.xml) separated by spaces or a directory that contains custom rules. |
| Fortify SCA scan filter file | Specify the name of a filter file. You can use a file to filter out specific vulnerability categories, rules, and vulnerability instances from the analysis. For more information, see the <i>Micro Focus Fortify Static Code Analyzer User Guide</i> . |

- To upload the scan results to Fortify Software Security Center:
 - Select the **Upload Fortify SCA scan results to Fortify Software Security Center** check box.
 - Specify an application name and application version.
If you have a successful connection to a Fortify Software Security Center server, you can select an application name and version from the list. Always specify both application name and application version.
- Click **Save**.

Creating a Post-Build Action to Translate Locally and Scan Remotely

To configure a post-build action to perform the translation phase on the local system and the scan phase on a remote system:

- From Jenkins, select an existing job to view or create a new job.
If you selected an existing job, click **Configure** on the job page.
- In the **Post-build Actions** section, click **Add post-build action**, and then select **Fortify Assessment**.
- Select **Local translation & remote scan**.
- To download Fortify security content:

Note: This setting only updates Fortify security content on the local system and is used for the local translation. Make sure that you have the same version of Fortify security content on the local system and on the remote system.

- a. Select the **Update Fortify Security Content** check box.
- b. In the **Update server URL** box, type the URL for the Fortify Rulepack update server.
The default Fortify Rulepack update server URL is `https://update.fortify.com`.

Note: To connect to the Fortify Rulepack update server with a proxy server, you need to configure Fortify security content update settings with the `scapostinstall` tool. For instructions, see the *Micro Focus Fortify Static Code Analyzer User Guide*.

5. In the **Build ID** box, type a unique identifier for the analysis.
6. (Optional) In the **Maximum heap memory** box, specify the maximum heap memory as an integer only.

For example, to specify 48 GB, type 49152. By default, Fortify Static Code Analyzer automatically allocates memory based on the physical memory available on the system. If you specify an amount of memory in this field, it overrides the default automatic memory allocation.
7. (Optional) In the **Additional JVM options** box, you can add JVM commands.
8. From the **Application type** list, select the type of application you want to analyze.

Note: Enclose each option and parameter in double quotes in boxes where you can specify multiple values.

For example: `"-build-label" "label" "-disable-source-bundling"`

Note: The Fortify Jenkins Plugin uses the PATH environment variable to find the executable for gradle, maven, devenv, and msbuild.

| Application Type | Description |
|--------------------------|---|
| .NET Devenv | <ol style="list-style-type: none"> a. In the Solution or project file box, type the solution or project file name (or the path to the file). b. (Optional) Specify any additional devenv options. |
| .NET MSBuild | <ol style="list-style-type: none"> a. In the Solution or project file box, type the solution or project file name (or the path to the file). b. (Optional) Specify any additional MSBuild options. |
| .NET source code scan | <ol style="list-style-type: none"> a. In the .NET framework version box, specify the .NET framework version used to compile the code. b. (Optional) In the Libdirs box, specify a semicolon-separated list of directories where referenced system or third-party DLLs are located. c. (Optional) In the Fortify SCA translation options box, specify any additional Fortify Static Code Analyzer translation options. See the <i>Micro Focus Fortify Static Code Analyzer User Guide</i> for detailed information |

| Application Type | Description |
|------------------|--|
| | <p>about the available translation options.</p> <p>d. In the Source files box, specify the source files to translate.</p> |
| Java | <p>Specify the Java source path, classpath, the source files, and any additional Fortify Static Code Analyzer translation options. The only required field is Source files. See the <i>Micro Focus Fortify Static Code Analyzer User Guide</i> for more detailed information about the Java translation options.</p> |
| Maven | <p>a. If you did not run the build previously, then in the Maven options box, type package. Otherwise, leave this box empty.</p> <div data-bbox="488 743 1403 926" style="background-color: #f0f0f0; padding: 10px;"> <p>Note: The translation log is in the /target directory that is created when the “package” runs from Maven. Any log file location specified in the Fortify Jenkins Plugin is ignored when the Fortify Maven Plugin performs the translation.</p> </div> |
| Gradle | <p>a. To use a Wrapper, select Use Gradle Wrapper.</p> <p>b. In the Gradle tasks box, type the Gradle tasks required for your project.</p> <p>c. In the Gradle options box, type the Gradle options required for your project.</p> |
| Other | <p>a. (Optional) Provide all the Fortify Static Code Analyzer translation options in the Fortify SCA translation options box. See the <i>Micro Focus Fortify Static Code Analyzer User Guide</i> for detailed information about the available translation options.</p> <p>b. Specify the source code to scan in the Includes list box.</p> |
| Advanced | <p>Select Advanced if you are familiar with the Fortify Static Code Analyzer command-line interface or you want to specify all the translation options without any guidance. Specify all the Fortify Static Code Analyzer translation options including source files. See the <i>Micro Focus Fortify Static Code Analyzer User Guide</i> for detailed information about the translation options.</p> |

9. (Optional) You can exclude files or directories from the translation by adding them to the **Exclude list** box.
10. (Optional) Enable the debug or verbose logging options.
11. (Optional) To specify CloudScan Controller settings, add Fortify Static Code Analyzer scan options, custom Rulepacks, or a scan filter file, click **Optional configuration**. The following table describes the optional configuration settings.

| Field | Description |
|------------------------------|--|
| Sensor pool | Specify a sensor pool UUID defined in Fortify Software Security Center. By default, Fortify CloudScan uses the default sensor pool as defined in Fortify Software Security Center. |
| Notification email | Specify the email address to which the Controller will send notifications. |
| Fortify SCA scan options | Specify Fortify Static Code Analyzer scan options. For descriptions of the available scan options, see the <i>Micro Focus Fortify Static Code Analyzer User Guide</i> . Note: Enclose each option and parameter in double quotes. In the following example, two analyzers and quick scan mode are enabled for the scan: <code>"-analyzers" "controlflow,dataflow" "-quick"</code> . |
| Custom Rulepacks | Specify custom rules files (*.xml) separated by spaces or a directory that contains custom rules. |
| Fortify SCA scan filter file | Specify the name of a filter file. You can use a file to filter out specific vulnerability categories, rules, and vulnerability instances from the analysis. For more information, see the <i>Micro Focus Fortify Static Code Analyzer User Guide</i> . |

12. To upload the scan results to Fortify Software Security Center:
 - a. Select the **Upload Fortify SCA scan results to Fortify Software Security Center** check box.
 - b. Specify an application name and an application version.

If you have a successful connection to a Fortify Software Security Center server, you can select an application name and version from the list. Always specify both application name and application version.
13. Click **Save**.

Creating a Post-Build Action to Translate and Scan Locally

To configure a post-build action to perform a complete analysis on the local system:

1. From Jenkins, select an existing job to view or create a new job.

If you selected an existing job, click **Configure** on the job page.
2. In the **Post-build Actions** section, click **Add post-build action**, and then select **Fortify Assessment**.
3. Select **Local translation & local scan**.

4. To download Fortify security content before the scan:
 - a. Select the **Update Fortify Security Content** check box.
 - b. In the **Update server URL** box, type the URL for the Fortify Rulepack update server.
The default Fortify Rulepack update server URL is `https://update.fortify.com`.

Note: To connect to the Fortify Rulepack update server with a proxy server, you need to configure Fortify security content update settings with the `scapostinstall` tool. For instructions, see the *Micro Focus Fortify Static Code Analyzer User Guide*.

5. In the **Build ID** box, type a unique identifier for the analysis.
6. (Optional) In the **Results file** box, type a name for the Fortify results file (FPR). For example, `MyProjectA.fpr`.

Note: You do not need to specify the `.fpr` file extension.

If you do not provide a results file name:

- If you are running a Fortify SCA scan, the analysis results are written to `scan.fpr` in the workspace.

Note: If this file already exists, it will be overwritten.

- If you are not running a Fortify SCA scan and you are uploading results to Fortify Software Security Center, Fortify Jenkins Plugin searches `./**/*.fpr` in the workspace for the FPR file with the latest modified date.
7. (Optional) In the **Maximum heap memory** box, specify the maximum heap memory as an integer only.

For example, to specify 48 GB, type `49152`. By default, Fortify Static Code Analyzer automatically allocates memory based on the physical memory available on the system. If you specify an amount of memory in this field, it overrides the default automatic memory allocation.

8. (Optional) In the **Additional JVM options** box, you can add JVM commands.
9. From the **Application type** list, select the type of application you want to analyze.

Note: Enclose each option and parameter in double quotes in boxes where you can specify multiple values.

For example: `"-build-label" "label" "-disable-source-bundling"`

Note: The Fortify Jenkins Plugin uses the `PATH` environment variable to find the executable for `gradle`, `maven`, `devenv`, and `msbuild`.

| Application Type | Description |
|-------------------------|---|
| .NET Devenv | <ul style="list-style-type: none"> a. In the Solution or project file box, type the solution or project file name (or the path to the file). b. (Optional) Specify any additional devenv options. |
| .NET MSBuild | <ul style="list-style-type: none"> a. In the Solution or project file box, type the solution or project file name (or the path to the file). b. (Optional) Specify any additional MSBuild options. |
| .NET source code scan | <ul style="list-style-type: none"> a. In the .NET framework version box, specify the .NET framework version used to compile the code. b. (Optional) In the Libdirs box, specify a semicolon-separated list of directories where referenced system or third-party DLLs are located. c. (Optional) In the Fortify SCA translation options box, specify any additional Fortify Static Code Analyzer translation options. See the <i>Micro Focus Fortify Static Code Analyzer User Guide</i> for detailed information about the available translation options. d. In the Source files box, specify the source files to translate. |
| Java | <p>Specify the Java source path, classpath, the source files, and any additional Fortify Static Code Analyzer translation options. The only required field is Source files. See the <i>Micro Focus Fortify Static Code Analyzer User Guide</i> for more detailed information about the Java translation options.</p> |
| Maven | <ul style="list-style-type: none"> a. If you did not run the build previously, then in the Maven options box, type package. Otherwise, leave this box empty. <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Note: The translation log is in the /target directory that is created when the “package” runs from Maven. Any log file location specified in the Fortify Jenkins Plugin is ignored when the Fortify Maven Plugin performs the translation.</p> </div> |
| Gradle | <ul style="list-style-type: none"> a. To use a Wrapper, select Use Gradle Wrapper. b. In the Gradle tasks box, type the Gradle tasks required for your project. c. In the Gradle options box, type the Gradle options required for your project. |

| Application Type | Description |
|-------------------------|--|
| Other | a. (Optional) Provide all the Fortify Static Code Analyzer translation options in the Fortify SCA translation options box. See the <i>Micro Focus Fortify Static Code Analyzer User Guide</i> for detailed information about the available translation options. b. Specify the source code to scan in the Includes list box. |
| Advanced | Select Advanced if you are familiar with the Fortify Static Code Analyzer command-line interface or you want to specify all the translation options without any guidance. Specify all the Fortify Static Code Analyzer translation options including source files. See the <i>Micro Focus Fortify Static Code Analyzer User Guide</i> for detailed information about the translation options. |

10. (Optional) You can exclude files or directories from the translation by adding them to the **Exclude list** box.
11. (Optional) Enable the debug or verbose logging options.
12. (Optional) To specify a custom location for the Fortify Static Code Analyzer log file, type a file name (or a full path) in the **Log file location** box.
By default, the log file is written to the workspace in `/.fortify/sca<version>/log`.
13. To run a scan, select the **Run Fortify SCA scan** check box, and then specify the scan settings:
 - a. (Optional) In the **Custom Rulepacks** box, specify custom rules.
Specify custom rules files (*.xml) separated by spaces or a directory that contains custom rules.
 - b. (Optional) Specify any additional scan options.

Note: Enclose each option and parameter in double quotes.

In the following example, two analyzers and quick scan mode are enabled for the scan:
`"-analyzers" "controlflow,dataflow" "-quick"`.

- c. (Optional) Enable the debug or verbose logging options.
- d. (Optional) To specify a custom location for the Fortify Static Code Analyzer log file, type a file name (or a full path) in the **Log file location** box.

By default, the log file is written to the workspace in `/.fortify/sca<version>/log`.

14. To upload the scan results to Fortify Software Security Center, select the **Upload Fortify SCA scan results to Fortify Software Security Center** check box, and then specify the upload settings:

- a. Specify an application name and an application version.

If you have a successful connection to a Fortify Software Security Center server, you can select an application name and version from the list. Always specify both application name and application version.

Note: If an application with the specified name and version does not exist on Fortify Software Security Center, Fortify Jenkins Plugin creates it for a successful build.

- b. (Optional) Specify the ID of a filter set to use when retrieving scan results for display in Jenkins. If no value is specified, the Fortify Jenkins Plugin uses the default filter set configured in Fortify Software Security Center.

The filter set ID for Quick View is 32142c2d-3f7f-4863-a1bf-9b1e2f34d2ed and the filter set ID for Security Auditor View is a243b195-0a59-3f8b-1403-d55b7a7d78e6.

The fail condition and the Normalized Vulnerability Score (NVS) calculation depend on the issues filtered by the filter set. For example, if a Quick View filter is applied to the project issues (and no critical or high issues are found), then the fail condition determines that there is no reason to set this build to “unstable” and the NVS is set to zero. The graph summary also shows zero.

- c. (Optional) To trigger a build failure based on scan results, type a search query in the **Build failure criteria** box.

For example, the following search query causes the build to fail if any critical issues exist in the scan results:

```
[fortify priority order]:critical
```

See the *Micro Focus Fortify Software Security Center User Guide* for a description of the search query syntax.

- d. (Optional) To specify the interval that the Fortify Jenkins Plugin polls Fortify Software Security Center to determine if the FPR processing is complete, click **Advanced settings**. In the **Polling interval** field, specify an interval (in minutes). The valid values are 0-60 and the default is 1 minute.

The Fortify Jenkins Plugin polls Fortify Software Security Center until the FPR is processed before it runs the NVS calculation.

Important! If the FPR processing requires approval, then this step will not complete until the approval is granted through Fortify Software Security Center.

15. Click **Save**.

Configuring Fortify Analysis with Pipeline Jobs

The Fortify Jenkins Plugin supports both Declarative and Scripted Pipeline syntax. The advantage of using Jenkins Pipeline is that you can check your script into source control, and you can have multiple Fortify Static Code Analyzer translation or upload requests (for example) within the same Jenkinsfile script. See the Jenkins documentation for additional information about pipelines.

Pipeline Steps to Translate and Scan Remotely

There are two Pipeline steps available to perform the analysis remotely. The following table lists these Fortify Jenkins Plugin Pipeline steps. Each section describes the parameters and contains examples.

| Task | Pipeline Step |
|--|--|
| Set options for remote translation and scan. This step is optional and if used should precede a <code>fortifyRemoteAnalysis</code> step. | "fortifyRemoteArguments Step" on page 29 |
| Send a project to a remote system for analysis. | "fortifyRemoteAnalysis Step" on page 29 |

The following is an example Jenkinsfile that sends a Java project that uses Gradle to a remote system for analysis. After the remote analysis is complete, the Controller uploads the analysis results to Fortify Software Security Center.

```
node {
  stage('Fortify Remote Arguments') {
    fortifyRemoteArguments transOptions: '-Xmx4G',
      scanOptions: '"-analyzers" "dataflow"'
  }
  stage('Fortify Remote Analysis') {
    fortifyRemoteAnalysis remoteAnalysisProjectType: fortifyGradle(),
      remoteOptionalConfig: [notifyEmail: 'joe@xyzCo.com',
        customRulepacks: 'MyRules.xml'],
      uploadSSC: [appName: 'MyJavaApp', appVersion: '3.1']
  }
}
```

The following Declarative Pipeline script has the same functionality as the previous example:

```
pipeline {
  agent any
  stages {
    stage('Fortify Remote Arguments') {
      steps {
        fortifyRemoteArguments transOptions: '-Xmx4G',
          scanOptions: '"-analyzers" "dataflow"'
      }
    }
    stage('Fortify Remote Analysis') {
      steps {
        fortifyRemoteAnalysis remoteAnalysisProjectType: fortifyGradle(),
          remoteOptionalConfig: [notifyEmail: 'joe@xyzCo.com',
            customRulepacks: 'MyRules.xml'],
          uploadSSC: [appName: 'MyJavaApp', appVersion: '3.1']
      }
    }
  }
}
```

fortifyRemoteArguments Step

Use this step to specify Fortify Static Code Analyzer translation and scan options in a settings file for remote analysis. This step is optional. To initiate a remote analysis, follow this step with a [fortifyRemoteAnalysis step](#) (see "[fortifyRemoteAnalysis Step](#)" below).

| Parameter | Description |
|--------------|---|
| transOptions | Optional (String). Specifies any additional Fortify Static Code Analyzer translation options. Enclose each option and parameter in double quotes. |
| scanOptions | Optional (String). Specifies any additional Fortify Static Code Analyzer scan options. Enclose each option and parameter in double quotes. |

fortifyRemoteArguments Example

The following example specifies 4 GB for the translation and excludes SQL. Only Control Flow and Dataflow analyzers are used and the default Rulepacks are not processed for the scan phase.

```
node {
  stage('Fortify Remote Arguments') {
    fortifyRemoteArguments transOptions: '"-Xmx4G"
    "-disable-language" "sql"',
    scanOptions: '"-analyzers" "controlflow,dataflow"
    "-no-default-rules"'
  }
}
```

fortifyRemoteAnalysis Step

Use this step to send a project to a remote system for analysis (translation and scan). To add additional translation or scan options for the analysis, precede this step with the [fortifyRemoteArguments step](#) (see "[fortifyRemoteArguments Step](#)" above).

| Parameter | Description | Default Value |
|---------------------------|--|---------------|
| RemoteAnalysisProjectType | Required (String). The application type is one of the following: fortifyGradle, fortifyMaven, fortifyPHP, fortifyPython, and fortifyOther. | |
| Gradle Parameters | | |

| Parameter | Description | Default Value |
|--|---|---------------|
| includeTests | Optional (boolean). Specifies whether to include a test source set. | false |
| buildFile | Optional (String). Specifies the build file name. | build.gradle |
| Maven Parameters | | |
| includeTests | Optional (boolean). Specifies whether to include a test scope. | false |
| buildFile | Optional (String). Specifies the build file name. | pom.xml |
| PHP Parameters | | |
| phpVersion | Optional (Number). Specifies the PHP version used in the project. | 7.0 |
| Python Parameters | | |
| pythonVersion | Optional (String). Specify the Python version used in the project. The valid values are 2 and 3. This parameter is ignored if you also provide the <code>pythonVirtualEnv</code> parameter. | 2 |
| pythonVirtualEnv | Optional (String). Specifies the location (directory) of the Python virtual environment. | (none) |
| pythonRequirementsFile | Optional (String). Specifies the Python project requirements file used to install and collect dependencies. | (none) |
| remoteOptionalConfig Parameters | | |
| sensorPoolUUID | Optional (String). Specifies the sensor pool to which to submit the job. | (none) |
| notifyEmail | Optional (String). Specifies the email address to which the Controller will send notifications. | (none) |
| customRulepacks | Optional (String). Specify custom rules files (*.xml) separated by spaces or a directory that contains custom rules. | |

| Parameter | Description | Default Value |
|-----------------------------|---|---------------|
| filterFile | Optional (String). Specifies a file used to filter out specific vulnerability categories, rules, and vulnerability instances from the analysis. For more information about filter files, see the <i>Micro Focus Fortify Static Code Analyzer User Guide</i> . | (none) |
| uploadSSC Parameters | | |
| appName | Required (String). Specifies an existing application name for which to store the results in Fortify Software Security Center. | |
| appVersion | Required (String). Specifies an existing application version for which to store the results in Fortify Software Security Center. | |

fortifyRemoteAnalysis Example

The following example uploads a Python 3 project to a remote system for translation and scan. Controller notifications are emailed to joe@xyzCo.com. After the analysis is complete, the project is uploaded to Fortify Software Security Center.

```
node {  
  stage('Get Src Code') {  
    git credentialsId: '3e58c50d-cd4a-6e28-ff44-cb164dec13f2',  
    url: 'https://github.xyzCo.com/MyDept/projA.git'  
  }  
  
  stage('Fortify Remote Analysis') {  
    fortifyRemoteAnalysis  
    remoteAnalysisProjectType: fortifyPython: (pythonVersion: '3',  
    pythonRequirementsFile: 'C:\\projA\\requirements.txt',  
    pythonVirtualEnv: 'C:\\projA\\my_project'),  
    remoteOptionalConfig: [notifyEmail: 'joe@xyzCo.com'],  
    uploadSSC: [appName: 'ProjA', appVersion: '2.3Beta']  
  }  
}
```

Pipeline Steps to Translate locally and Scan Remotely

The following table lists the available Fortify Jenkins Plugin Pipeline steps to perform local translation, remote scan, and upload to Fortify Software Security Center. Each section describes the parameters and contains examples.

| Project Build Step | Pipeline Step |
|-------------------------------------|---|
| Run a local Fortify SCA clean | "fortifyClean Step" on page 38 |
| Run a local Fortify SCA translation | "fortifyTranslate Step" on page 39 |
| Run a Remote Fortify SCA scan | "fortifyRemoteScan Step" on the next page |

Note: If any Fortify Jenkins Plugin Pipeline step in a script fails to execute, then the build fails. You do have the option to implement your own exception-catch mechanism to ignore a step failure.

The following is an example Jenkinsfile that performs the Fortify Static Code Analyzer translation for a Java project on the local system, uploads the project to a remote system for scanning, and then uploads the analysis results to Fortify Software Security Center:

```
node {
  stage('Fortify Clean') {
    fortifyClean buildID: 'MyJavaApp', logFile: 'MyJavaAppFortify.log'
  }
  stage('Fortify Translate') {
    fortifyTranslate buildID: 'MyJavaApp',
    logFile: 'MyJavaApp-translate.log',
    projectScanType: fortifyJava(javaSrcFiles:
    'src\\main\\java\\com\\projectA',
    javaVersion: '11')
  }
  stage('Remote Fortify Scan Upload to SSC') {
    fortifyRemoteScan buildID: 'MyJavaApp',
    remoteOptionalConfig: [notifyEmail: 'joe@xyzCo.com',
    scanOptions:"-analyzers" "controlflow"],
    uploadSSC: [appName: 'JavaAppA', appVersion: '3']
  }
}
```


The following Declarative Pipeline script has the same function as the previous example:

```
pipeline {
  agent any
  stages {
    stage('Fortify Clean') {
      steps {
        fortifyClean buildID: 'MyJavaApp',
          logfile: 'MyJavaAppFortify.log'
      }
    }
    stage('Fortify Translate') {
      steps {
        fortifyTranslate buildID: 'MyJavaApp',
          logfile: 'MyJavaApp-translate.log',
          projectScanType: fortifyJava(javaSrcFiles:
            'src\\main\\java\\com\\projectA', javaVersion: '11')
      }
    }
    stage('Remote Fortify Scan Upload to SSC') {
      steps {
        fortifyRemoteScan buildID: 'MyJavaApp',
          remoteOptionalConfig: [notifyEmail: 'joe@xyzCo.com',
            scanOptions:"-analyzers" "controlflow"],
          uploadSSC: [appName: 'JavaAppA', appVersion: '3']
      }
    }
  }
}
```

fortifyRemoteScan Step

Use this step to send a locally translated project to a remote system for the scan phase.

| Parameter | Description | Default Value |
|--|--|---------------|
| buildID | Required (String). A unique identifier for the analysis. | |
| remoteOptionalConfig Parameters | | |
| sensorPoolUUID | Optional (String). Specifies the sensor pool to which to submit the job. | (none) |

| Parameter | Description | Default Value |
|-----------------------------|---|---------------|
| notifyEmail | Optional (String). Specifies the email address to which the Controller will send notifications. | (none) |
| scanOptions | Optional (String). Fortify Static Code Analyzer scan options. For descriptions of the available scan options, see the <i>Micro Focus Fortify Static Code Analyzer User Guide</i> . Note: Enclose each option and parameter in double quotes. In the following example, two analyzers and quick scan mode are enabled for the scan: "- analyzers" "controlflow,dataflow" "-quick". | (none) |
| customRulepacks | Optional (String). Specify custom rules files (*.xml) separated by spaces or a directory that contains custom rules. | (none) |
| filterFile | Optional (String). Specifies a file used to filter out specific vulnerability categories, rules, and vulnerability instances from the analysis. For more information about filter files, see the <i>Micro Focus Fortify Static Code Analyzer User Guide</i> . | (none) |
| uploadSSC Parameters | | |
| appName | Required (String). Specifies an existing application name for which to store the results in Fortify Software Security Center. | |
| appVersion | Required (String). Specifies an existing application version for which to store the results in Fortify Software Security Center. | |

fortifyRemoteScan Example

The following example uploads a locally translated project with a build ID of MyAppA to the remote system for scanning. After the scan is complete, the project is uploaded to Fortify Software Security Center.

```
node {  
  stage('Remote Fortify Scan Upload to SSC') {  
    fortifyRemoteScan buildID: 'MyAppA',  
    remoteOptionalConfig: [notifyEmail: 'joe@xyzCo.com',  
    scanOptions:"-quick"],  
    uploadSSC: [appName: 'AppA', appVersion: 'version1']  
  }  
}
```

Pipeline Steps to Translate and Scan Locally

The following table lists the available Fortify Jenkins Plugin Pipeline steps to update Fortify security content, run a local translation, run a local scan, and upload analysis results to Fortify Software Security Center. Each section describes the parameters and contains examples.

| Project Build Step | Pipeline Step |
|---|--|
| Update Fortify security content to use for local translation and scan | "fortifyUpdate Step" on page 38 |
| Run a local Fortify SCA clean | "fortifyClean Step" on page 38 |
| Run a local Fortify SCA translation | "fortifyTranslate Step" on page 39 |
| Run a local Fortify SCA scan | "fortifyScan Step" on page 44 |
| Upload local Fortify SCA scan results to Fortify Software Security Center | "fortifyUpload Step" on page 46 |

Note: If any Fortify Jenkins Plugin Pipeline step in a script fails to execute, then the build fails. You do have the option to implement your own exception-catch mechanism to ignore a step failure.

The following is an example Jenkinsfile that updates Fortify security content, performs a complete Fortify analysis of a Java project, and then uploads the analysis results to Fortify Software Security Center:

```
node {
  stage('Fortify Update') {
    fortifyUpdate updateServerURL: 'https://update.fortify.com'
  }
  stage('Fortify Clean') {
    fortifyClean buildID: 'MyJavaApp', logFile: 'MyJavaAppFortify.log'
  }
  stage('Fortify Translate') {
    fortifyTranslate buildID: 'MyJavaApp',
    logFile: 'MyJavaApp-translate.log',
    projectScanType: fortifyJava(javaSrcFiles:
      'src\\main\\java\\com\\projectA', javaVersion: '11')
  }
  stage('Fortify Scan') {
    fortifyScan buildID: 'MyJavaApp', resultsFile: 'MyJavaApp.fpr'
    customRulepacks: 'MyRules.xml', logFile: 'MyJavaApp-scan.log'
  }
  stage('Fortify Upload') {
    fortifyUpload appName: 'JavaAppA', appVersion: '3',
    resultsFile: 'MyJavaApp.fpr'
  }
}
```

The following Declarative Pipeline script has the same function as the previous example:

```
pipeline {
  agent any
  stages {
    stage('Fortify Update') {
      steps {
        fortifyUpdate updateServerURL: 'https://update.fortify.com'
      }
    }
    stage('Fortify Clean') {
      steps {
        fortifyClean buildID: 'MyJavaApp',
          logfile: 'MyJavaAppFortify.log'
      }
    }
    stage('Fortify Translate') {
      steps {
        fortifyTranslate buildID: 'MyJavaApp',
          logfile: 'MyJavaApp-translate.log',
          projectScanType: fortifyJava(javaSrcFiles:
            'src\\main\\java\\com\\projectA', javaVersion: '11')
      }
    }
    stage('Fortify Scan') {
      steps {
        fortifyScan buildID: 'MyJavaApp',
          resultsFile: 'MyJavaApp.fpr'
          customRulepacks: 'MyRules.xml',
          logfile: 'MyJavaApp-scan.log'
      }
    }
    stage('Fortify Upload') {
      steps {
        fortifyUpload appName: 'JavaAppA', appVersion: '3',
          resultsFile: 'MyJavaApp.fpr'
      }
    }
  }
}
```

fortifyUpdate Step

Use this step to update the local copy of the Fortify security content used by the Fortify translation and scan steps.

| Parameter | Description | Default Value |
|-----------------|--|----------------------------|
| updateServerURL | Optional (String). Specifies the URL for the Fortify Rulepack update server. | https://update.fortify.com |

fortifyUpdate Example

The following example updates the Fortify security content:

```
node {
  stage('Fortify Update') {
    fortifyUpdate updateServerURL: 'https://update.fortify.com'
  }
}
```

fortifyClean Step

Use this step to remove any temporary files from a previous scan for a specific build ID.

| Parameter | Description | Default Value |
|---------------|---|---|
| buildID | Required (String). A unique identifier for the scan. | |
| maxHeap | Optional (int). The maximum heap size for the JVM (-Xmx). | By default, Fortify Static Code Analyzer automatically allocates memory based on the physical memory available on the system. |
| addJVMOptions | Optional (String). Specifies additional JVM commands. | (none) |
| debug | Optional (boolean). Specifies whether to include debug information in the Fortify Support log file. | false |
| verbose | Optional (boolean). Specifies whether to send verbose status messages to | false |

| Parameter | Description | Default Value |
|-----------|---|--|
| | the console and to the Fortify Support log file. | |
| logFile | Optional (String). Specifies the log file location and file name. | The default file name is sca.log and the default location is in the workspace directory. |

fortifyClean Example

The following example removes all the temporary files for the MyJavaApp build ID:

```
node {
  stage('Fortify Clean') {
    fortifyClean buildID: 'MyJavaApp', logFile: 'MyJavaAppFortify.log'
  }
}
```

fortifyTranslate Step

Use this step to translate the project source code on the local system.

| Parameter | Description | Default Value |
|---------------------------|--|---|
| General Parameters | | |
| buildID | Required (String). A unique identifier for the analysis. | |
| projectScanType | Required. (String). The project scan type is one of the following: fortifyAdvanced, fortifyDevenv, fortifyDotnetSrc, fortifyGradle, fortifyJava, fortifyMaven3, fortifyMSBuild, or fortifyOther. | |
| maxHeap | Optional (int). The maximum heap size for the JVM (-Xmx). | By default, Fortify Static Code Analyzer automatically allocates memory based on the physical memory available on the |

| Parameter | Description | Default Value |
|------------------------|---|---|
| | | system. |
| addJVMOptions | Optional (String). Additional JVM commands. | (none) |
| debug | Optional (boolean). Specifies whether to include debug information in the Fortify Support log file. | false |
| verbose | Optional (boolean). Specifies whether to send verbose status messages to the console and to the Fortify Support log file. | false |
| logFile | Optional (String). Specifies the log file location and file name. | The default file name is <code>sca.log</code> and the default location is the workspace directory. |
| excludeList | Optional (String). Specifies a list of directories or files to exclude from translation. | (none) |
| Java Parameters | | |
| javaSrcFiles | Required (String). Specifies the location of the Java source files. | |
| javaVersion | Optional (String). Specifies the JDK version for which the Java code is written. | The default version defined by Fortify Static Code Analyzer. For example, in Fortify Static Code Analyzer version 18.20, the default JDK version is 1.8. See the <i>Micro Focus Fortify Static Code Analyzer User Guide</i> for specific version information. |
| javaClasspath | Optional (String). Specifies the class path as a colon- or semicolon-separated list of | (none) |

| Parameter | Description | Default Value |
|------------------------------------|---|---------------|
| | directories to use for analyzing Java source code. | |
| javaAddOptions | Optional (String). Specifies any additional Fortify Static Code Analyzer options for translating Java code. | (none) |
| devenv / MSBuild Parameters | | |
| dotnetProject | Required (String). Specifies a solution (.sln) or a project (.proj) file. | |
| dotnetAddOptions | Optional (String). Specifies any additional Fortify Static Code Analyzer options for translating .NET code. | (none) |
| DotnetSrc Parameters | | |
| dotnetFrameworkVersion | Required (int). Specifies the .NET framework version. | |
| dotnetSrcFiles | Required (String). Specifies the location of the .NET source files. | |
| dotnetLibdirs | Optional (String). Specifies a semicolon-separated list of directories where referenced system or third-party DLLs are located. | (none) |
| dotnetAddOptions | Optional (String). Specifies any additional devenv or MSBuild options required for your project. | (none) |
| Maven3 Parameters | | |
| mavenOptions | Optional (String). Specifies | (none) |

| Parameter | Description | Default Value |
|----------------------------|--|---------------|
| | any additional Maven options required for your project. | |
| Gradle Parameters | | |
| gradleTasks | Required (String). Specifies the Gradle tasks required for your project. | |
| useWrapper | Optional (boolean). Specifies whether to use a Wrapper. | false |
| gradleOptions | Optional (String). Specifies any additional Gradle options required for your project. | (none) |
| Other Parameters | | |
| otherIncludesList | Required (String). Specifies the location of the source files. | |
| otherOptions | Optional (String). Specifies any additional Fortify Static Code Analyzer options required for your project. | (none) |
| Advanced Parameters | | |
| advOptions | Required (String). Specifies all the Fortify Static Code Analyzer options that are necessary to translate the project. | |

fortifyTranslate Examples

Specify a function name for the projectScanType parameter. The valid function names are: fortifyAdvanced(), fortifyDevenv(), fortifyDotnetSrc(), fortifyGradle(), fortifyJava(), fortifyMaven3(), fortifyMSBuild(), fortifyOther().

The following example translates a Java project and excludes some files from the translation:

```
node {
  stage('Fortify Translate') {
    fortifyTranslate buildID: 'MyJavaApp',
    excludeList: '"src\\main\\java\\com\\projectA\\command\\Config.java"
    "src\\main\\java\\com\\projectA\\command\\Test*.java"',
    logfile: 'MyJavaApp-translate.log',
    projectScanType: fortifyJava(javaSrcFiles:
    'src\\main\\java\\com\\projectA',javaVersion: '1.8')
  }
}
```

The following example uses Maven to translate a Java project:

```
node {
  stage('Fortify Translate') {
    fortifyTranslate buildID: 'MyJavaApp',
    excludeList: '"src\\main\\java\\com\\projectA\\command\\Config.java"
    "src\\main\\java\\com\\projectA\\command\\Test*.java"',
    logfile: 'MyJavaApp.log', maxHeap: '4800',
    projectScanType: fortifyMaven3(mavenOptions: 'package')
  }
}
```

The following example uses MSBuild to translate a .NET solution:

```
node {
  stage('Fortify Translate') {
    fortifyTranslate buildID: 'MyDotNetApp', ,
    logfile: 'MyJavaApp.log', maxHeap: '4800',
    projectScanType: fortifyMSBuild(dotnetProject: 'MyDotNetApp.sln',
    dotnetAddOptions: '/t:rebuild')
  }
}
```

The following example translates a Python 3 project:

```
node {
  stage('Fortify Translate') {
    fortifyTranslate buildID: 'MyPythonApp',
    excludeList: '"src\\**\\Test*.py"',
    logfile: 'MyPythonApp-translate.log',
    projectScanType: fortifyAdvanced(advOptions: '"-python-version" "3"
    "-python-path" "C:\\Python33\\lib\\site-packages"
    "src\\main\\pythonApp" ')
  }
}
```

The following example translates a JavaScript application:

```
node {
  stage ('Fortify Translate') {
    fortifyTranslate buildID: 'JS_App',
    logfile: 'JS_App-translate.log', projectScanType:
    fortifyOther(otherIncludesList: './**/*.js')
  }
}
```

fortifyScan Step

Use this step to run a scan on all the translated files with the specific build ID.

| Parameter | Description | Default Value |
|---------------|--|---|
| buildID | Required (String). A unique identifier for the scan. | |
| maxHeap | Optional (number). The maximum heap size for the JVM (-Xmx). | By default, Fortify Static Code Analyzer automatically allocates memory based on the physical memory available on the system. |
| addJVMOptions | Optional (String). Specifies additional JVM commands. | (none) |
| resultsFile | Optional (String). Specifies a name for the Fortify results file (FPR). For example, MyProjectA.fpr. | scan.fpr |

| Parameter | Description | Default Value |
|-----------------|---|--|
| customRulepacks | Optional (String). Specifies custom rules (XML files). | (none) |
| addOptions | Optional (String). Specifies any additional scan options. Enclose each option and parameter in double quotes. | (none) |
| debug | Optional (boolean). Specifies whether to include debug information in the Fortify Support log file. | false |
| verbose | Optional (boolean). Specifies whether to send verbose status messages to the console and to the Fortify Support log file. | false |
| logFile | Optional (String). Specifies the log file location and file name. | The default file name is <code>sca.log</code> and the default location is the workspace directory. |

fortifyScan Example

The following example scans the previously-translated project with the MyJavaApp build ID:

```
node {
  stage('Fortify Scan') {
    fortifyScan buildID: 'MyJavaApp', resultsFile: 'MyJavaApp.fpr'
    customRulepacks: 'MyRules.xml', logFile: 'MyJavaApp-scan.log'
  }
}
```

fortifyUpload Step

Use this step to upload the results of a Fortify analysis (FPR) to Micro Focus Fortify Software Security Center. The information to connect to Fortify Software Security Center is obtained from the **Fortify Assessment** section in the Jenkins global settings (see ["Configuring Global Settings for the Fortify Jenkins Plugin" on page 14](#)). After an upload you can view results the results in Jenkins (see ["Viewing Analysis Results" on the next page](#)).

| Parameter | Description | Default Value |
|-----------------|--|--|
| appName | Required (String). Specifies the application name for which to store the results in Fortify Software Security Center. | |
| appVersion | Required (String). Specifies the application version for which to store the results in Fortify Software Security Center. | |
| resultsFile | Optional (String). Specifies a name for the Fortify results file (FPR). For example, MyProjectA.fpr. | If you ran a Fortify SCA scan, the default file is scan.fpr, otherwise the Fortify Jenkins Plugin searches <code>"/**/*.fpr"</code> in the workspace for the FPR file with the latest modified date. |
| filterSet | Optional (String). Specifies the ID of a filter set to use when retrieving scan results for display in Jenkins. The filter set ID for Quick View is 32142c2d-3f7f-4863-a1bf-9b1e2f34d2ed and the filter set ID for Security Auditor View is a243b195-0a59-3f8b-1403-d55b7a7d78e6. | The default filter set configured in Fortify Software Security Center. |
| failureCriteria | Optional (String). Specifies a search query to use on the scan results to trigger a build failure. For example, <code>[fortify priority order]:critical</code> . | (none) |
| pollingInterval | Optional (int). Specifies the interval (in minutes) that the Fortify Jenkins Plugin | 1 |

| Parameter | Description | Default Value |
|-----------|---|---------------|
| | <p>polls Fortify Software Security Center to determine if the FPR processing is complete. The valid values are 0-60.</p> <p>Important! If the FPR processing requires approval, then this step will not complete until the approval is granted through Fortify Software Security Center.</p> | |

fortifyUpload Example

The following example uploads the Fortify analysis results for the MyJavaApp project to version 3 of the MyJavaApp application on Fortify Software Security Center:

```
node {
  stage('Fortify Upload') {
    fortifyUpload appName: 'MyJavaApp', appVersion: '3',
    resultsFile: 'MyJavaApp.fpr'
  }
}
```

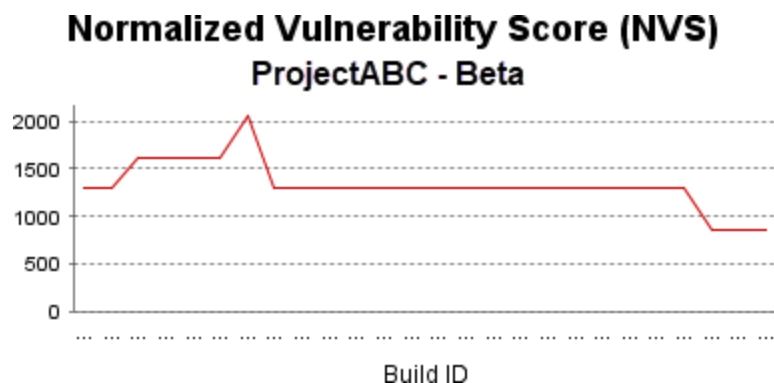
Viewing Analysis Results

When you perform the Fortify analysis on the local system and if you uploaded Micro Focus Fortify Static Code Analyzer results to Micro Focus Fortify Software Security Center, you can view a security vulnerability graph for your project and a summary of the issues from Jenkins.

Note: When an analysis is performed on a remote system and you uploaded the Fortify Static Code Analyzer results to Fortify Software Security Center, you can view the results in Fortify Software Security Center.

Security Vulnerability Graph for Your Project

The project page displays a Normalized Vulnerability Score (NVS) graph. The NVS is a normalized score that gives you a rough idea of the security vulnerability of your project.



The Fortify Jenkins Plugin calculates the NVS with the following formula:

$$\text{NVS} = ((\text{CFPO} * 10) + (\text{HFPO} * 5) + (\text{MFPO} * 1) + (\text{LFPO} * 0.1)) * 0.5 + ((\text{P1} * 2) + (\text{P2} * 4) + (\text{P3} * 16) + (\text{PABOVE} * 64)) * 0.5$$

where:

- CFPO = Number of critical vulnerabilities (unless audited as Not an Issue)
- HFPO = Number of high vulnerabilities (unless audited as Not an Issue)
- MFPO = Number of medium vulnerabilities (unless audited as Not an Issue)
- LFPO = Number of low vulnerabilities (unless audited as Not an Issue)

and:

- PABOVE = Exploitable
- P3 = Suspicious
- P2 = Bad practice
- P1 = Reliability issue

The total issues count is not very useful. For example, if Application A has no critical issues and ten low issues, the total issue count is ten. If Application B has five critical issues and no low issues, the total issue count is five. These values might mislead you to think that Application B is less vulnerable than Application A, when it is not.

The NVS calculated for the two example applications provides a different picture (simplified equation):

- Application A: $\text{NVS} = 0 * 10 + 10 * 0.1 = 1$
- Application B: $\text{NVS} = 5 * 10 + 0 * 0.1 = 50$

Viewing Issues

To see the issues for a Fortify Static Code Analyzer analysis that you have uploaded to Micro Focus Fortify Software Security Center, open your job in Jenkins and click **Fortify Assessment** on the left.

The interactive **List of Fortify SSC issues** page displays the **Summary** and **Issues breakdown by Priority Order** tables.

List of Fortify SSC issues

Summary

| Build | Total | Critical | High | Medium | Low |
|---------|---------|----------|-------|--------|---------|
| #7 (#0) | 77 (77) | 0 (0) | 4 (4) | 0 (0) | 73 (73) |

Issues breakdown by Priority Order

Critical (0) High (4) Medium (0) Low (73) **All (1 to 50 out of 77)**

| Primary Location | Category |
|--------------------------------------|---------------------------------------|
| Exec.java:292 | Command Injection |
| Exec.java:103 | Command Injection |
| Exec.java:202 | Dead Code: Expression is Always false |
| Exec.java:150 | Dead Code: Expression is Always false |
| Exec.java:111 | Dead Code: Expression is Always false |
| Exec.java:118 | Dead Code: Expression is Always true |
| Exec.java:418 | Denial of Service |
| Exec.java:229 | Denial of Service |
| ExecResults.java:335 | Denial of Service: StringBuilder |

The **Summary** table shows the difference in the number of issues in different categories between the two most recent builds. A blue arrow next to a value indicates that the number in that category has decreased, and a red arrow indicates that the number in that category has increased.

The **Issues breakdown by Priority Order** table shows detailed information about the issues for the specified location and category in each priority folder. Wait for the table to load. If the data load takes longer than expected, you might need to refresh the browser window.

By default, you see the critical issues first. To see all issues, click the **All** tab.

Note: The more issues a page shows, the longer it takes to load. Fortify recommends that you not use the **All** tab for large projects.

The first and the second columns show the file name and line number of the issue and the full path to this file. The last column displays the category of each vulnerability.

By default, issues are sorted by primary location. To organize them by category, click the **Category** column header.

To see more details about or to audit a specific issue, click the file name in the first column. The link takes you directly to the details for that issue on the Fortify Software Security Center server. If you are not logged in to Fortify Software Security Center, you are prompted to log in.

Configuring the Number of Issues Displayed on a Page

By default, the page displays up to 50 issues. To navigate to all the issues, use **Next>>** and **<<Previous** on the top and bottom of the table. To increase the maximum number of issues displayed to 100 per page, from the **50 | 100 | All** section at the bottom of the page, click **100**.

To control the number of the issues shown on a page from the **Configure System** page:

- In the **Fortify Assessment** section, change the value in the **Maximum issues per page** box.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on User Guide (Fortify Jenkins Plugin 19.2.0)

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@microfocus.com.

We appreciate your feedback!