

Fortify SCA Jenkins Plugin

19.1.0

Jonathan Couch
Fortify Security Support Engineer



Downloading Jenkins plugin (latest)

- Download the latest version from the following github repository <https://github.com/jenkinsci/fortify-plugin>
- Select the Master branch and download

Fortify Jenkins plugin <https://plugins.jenkins.io/fortify>

fortify fortify-sca security jenkins-plugin security-pipeline security-automation security-tools

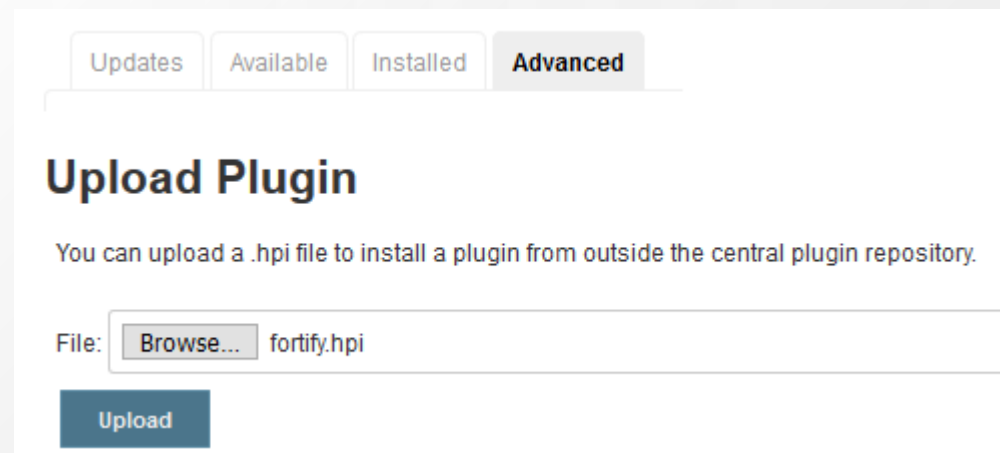
41 commits 1 branch 1 release 4 contributors View license

Branch: master New pull request Find File Clone or download

- Requires Maven and JDK to build the Jenkins plugin and uses the version that is supported by SCA 19.1.0 found in the system requirement guide.
- This will generate a fortify.hpi file containing the SCA Jenkins plugin



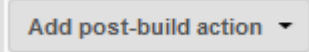
Installing the plugin

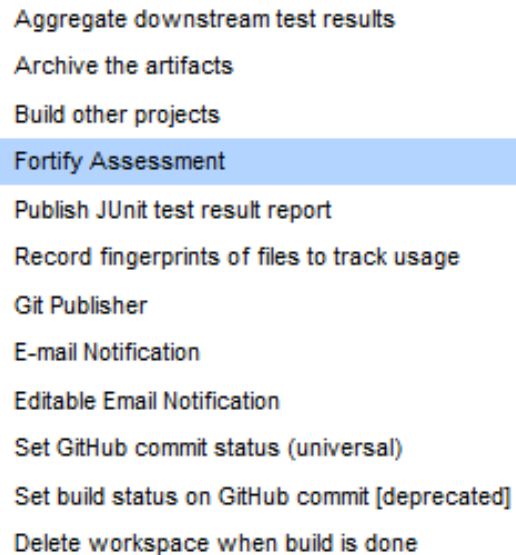
- Open Jenkins and navigate to Manage Jenkins -> Manage Plugins
- Switch to the Advanced tab and under the “Upload Plugin” section click the Browse button and select the generated fortify.hpi file



Configuring the Jenkins plugin

After successfully installing the plugin, it is ready to be used in a job.

- For an existing job, click on Configure eg  Configure
- Scroll down to the “Post-build actions” section eg 
- Click the “Add post-build action” dropdown and select “Fortify Assessment” 



Aggregate downstream test results
Archive the artifacts
Build other projects
Fortify Assessment
Publish JUnit test result report
Record fingerprints of files to track usage
Git Publisher
E-mail Notification
Editable Email Notification
Set GitHub commit status (universal)
Set build status on GitHub commit [deprecated]
Delete workspace when build is done

Configuring the Jenkins plugin (continued)

This will bring up the following field parameters and checkboxes. Enter the information needed to run a job.

Post-build Actions

Fortify Assessment X

Build ID ?

Results file ?

Maximum heap memory (MB) ?

Additional JVM options ?

Update Fortify Security Content ?

Run Fortify SCA clean

Run Fortify SCA translation ?

Run Fortify SCA scan

Upload Fortify SCA scan results to Fortify Software Security Center

Add post-build action ▼

Configuring the Jenkins plugin (continued)

Depending on the language to be scanned which can be either, Java, Maven, Gradle, or .NET, here are some examples.

The screenshot shows the 'Post-build Actions' configuration for the 'Fortify Assessment' plugin. The 'Build ID' field is set to `${JOB_NAME}_${BUILD_NUMBER}` and the 'Results file' field is set to `${JOB_NAME}_${BUILD_NUMBER}.FPR`. The 'Application type' dropdown menu is open, showing options: Java (selected), .NET, Maven 3, Gradle, and Other. Other fields include 'Maximum heap memory (MB)', 'Additional JVM options', 'Update Fortify Security Content' (unchecked), 'Run Fortify SCA clean' (checked), 'Run Fortify SCA translation' (checked), 'Translation type' (Basic), 'Fortify SCA translation options', 'Exclude list', 'Debug' (unchecked), 'Verbose' (unchecked), 'Log file location', 'Run Fortify SCA scan' (unchecked), and 'Upload Fortify SCA scan results to Fortify Software Security Center' (unchecked). At the bottom, there are 'Save' and 'Apply' buttons.

The fields can use Jenkins System Environment variables
Eg `${JOB_NAME}`, `${BUILD_NUMBER}`

Configuring the Jenkins plugin (continued)

Post-build Actions

Fortify Assessment x

Build ID

Results file

Maximum heap memory (MB)

Additional JVM options

Update Fortify Security Content

Run Fortify SCA clean

Run Fortify SCA translation

Translation type

Application type

Java source version

Java classpath

Source files

Fortify SCA translation options

Exclude list

Debug

Verbose

Log file location

Run Fortify SCA scan

Custom Rulepacks

Fortify SCA scan options

Debug

Verbose

Log file location

Upload Fortify SCA scan results to Fortify Software Security Center

Add post-build action

Java Example

Configuring the Jenkins plugin (continued)

Post-build Actions

Fortify Assessment

Build ID:

Results file:

Maximum heap memory (MB):

Additional JVM options:

Update Fortify Security Content

Run Fortify SCA clean

Run Fortify SCA translation

Translation type:

Application type:

Maven options:

Exclude list:

Debug

Verbose

Log file location:

Run Fortify SCA scan

Custom Rulepacks:

Fortify SCA scan options:

Debug

Verbose

Log file location:

Upload Fortify SCA scan results to Fortify Software Security Center

Add post-build action

Save Apply

Maven Example

Configuring the Jenkins plugin (continued)

Post-build Actions

Fortify Assessment

Build ID:

Results file:

Maximum heap memory (MB):

Additional JVM options:

Update Fortify Security Content

Run Fortify SCA clean

Run Fortify SCA translation

Translation type:

Application type:

Use Gradle Wrapper

Gradle tasks:

Gradle options:

Exclude list:

Debug

Verbose

Log file location:

Run Fortify SCA scan

Custom Rulepacks:

Fortify SCA scan options:

Debug

Verbose

Log file location:

Upload Fortify SCA scan results to Fortify Software Security Center

Add post-build action

Gradle Example

Configuring the Jenkins plugin (continued)

Post-build Actions

Fortify Assessment

Build ID:

Results file:

Maximum heap memory (MB):

Additional JVM options:

Update Fortify Security Content

Run Fortify SCA clean

Run Fortify SCA translation

Translation type:

Application type:

Scan type:

Build type:

Solution or project file:

devenv options:

Exclude list:

Debug

Verbose

Log file location:

Run Fortify SCA scan

Upload Fortify SCA scan results to Fortify Software Security Center

Add post-build action

Save Apply

.NET Example

Jenkins Pipeline

Pipeline

Definition Pipeline script

Script

```
1 pipeline {
2   agent any
3   environment {
4     PATH="C:\\_FORTIFY\\Fortify_SCA_and_Apps_19.1.0\\bin;%PATH%"
5   }
6   stages {
7     stage('fortify clean') {
8       steps{
9         echo 'Cleaning'
10        fortifyClean buildID: '${JOB_NAME}_${BUILD_NUMBER}'
11      }
12    }
13    stage('fortify Translate') {
14      steps{
15        echo 'Translating'
16        fortifyTranslate buildID: '${JOB_NAME}_${BUILD_NUMBER}',
17      }
18    }
19  }
```

Use Groovy Sandbox

[Pipeline Syntax](#) Clicking this will open a new tab where you can generate a pipeline script

Save **Apply**

Pipeline Example

Jenkins Pipeline (continued)

Overview

This **Snippet Generator** will help you learn the Pipeline Script code which can be used to define various steps. Pick a step you are interested in from the list, configure it, click **Generate Pipeline Script**, and you will see a Pipeline Script statement that would call the step with that configuration. You may copy and paste the whole statement into your script, or pick up just the options you care about. (Most parameters are optional and can be omitted in your script, leaving them at default values.)

Steps

Sample Step

Build ID

Application type

Java source version

Java classpath

Source files

Fortify SCA translation options

Exclude list

Generate Pipeline Script

```
fortifyTranslate addJVMOptions: "", buildID: "${JOB_NAME}_${BUILD_NUMBER}", excludeList: "", logFile: "", maxHeap: "", projectScanType: fortifyJava(javaAddOptions: "", javaClasspath: "", javaSrcFiles: 'C:\\_FORTIFY\\_\\Fortify_SCA_and_Apps_19.1.0\\Samples\\_\\basic\\_\\eightball\\_\\EightBall.java', javaVersion: '1.8')
```

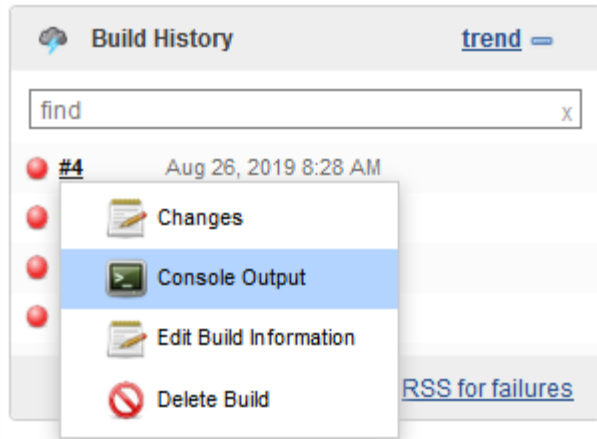
Global Variables

There are many features of the Pipeline that are not steps. These are often exposed via global variables, which are not supported by the snippet generator. See the [Global Variables Reference](#) for details.

Troubleshooting

When something goes wrong

Step 1: Check the console output



Troubleshooting

Console Output

When something goes wrong

Step 1: Check the console output

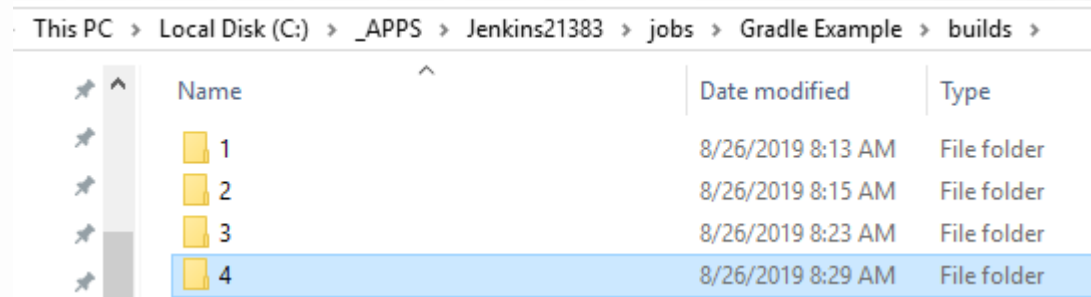
```
Started by user unknown or anonymous
Building in workspace C:\_apps\Jenkins21383\workspace\Gradle Example
Fortify Jenkins plugin v 19.1.30-SNAPSHOT (private-08/12/2019 14:27-pinaroc)
Fortify Jenkins plugin v 19.1.30-SNAPSHOT (private-08/12/2019 14:27-pinaroc)
Launching Fortify SCA clean command
found executable: C:\_FORTIFY\Fortify_SCA_and_Apps_19.1.0\bin\sourceanalyzer.exe
[Gradle Example] $ C:\_FORTIFY\Fortify_SCA_and_Apps_19.1.0\bin\sourceanalyzer.exe
"-Dcom.fortify.sca.ProjectRoot=C:\_apps\Jenkins21383\workspace\Gradle Example\.fortify" -clean -b "Gradle Example-4"
SCA clean returned exitcode=0
Fortify Jenkins plugin v 19.1.30-SNAPSHOT (private-08/12/2019 14:27-pinaroc)
Launching Fortify SCA translate command
found executable: C:\_FORTIFY\Fortify_SCA_and_Apps_19.1.0\bin\sourceanalyzer.exe
Running Gradle translation
found executable: C:\_APPS\GRADLE\gradle-4.9\bin\gradle.bat
[Gradle Example] $ C:\_FORTIFY\Fortify_SCA_and_Apps_19.1.0\bin\sourceanalyzer.exe
"-Dcom.fortify.sca.ProjectRoot=C:\_apps\Jenkins21383\workspace\Gradle Example\.fortify" -b "Gradle Example-4" C:\_APPS
\GRADLE\gradle-4.9\bin\gradle.bat -P C:\_FORTIFY\Fortify_SCA_and_Apps_19.1.0\Samples\advanced\BugTrackerPluginAlm clean
build
Starting a Gradle Daemon (subsequent builds will be faster)
starting init script
TaskListener registered.
> Task :clean UP-TO-DATE
> Task :compileJava NO-SOURCE
> Task :processResources NO-SOURCE
> Task :classes UP-TO-DATE
> Task :jar
> Task :assemble
> Task :compileTestJava NO-SOURCE
> Task :processTestResources NO-SOURCE
> Task :testClasses UP-TO-DATE
> Task :test NO-SOURCE
> Task :check UP-TO-DATE
> Task :build
```

Troubleshooting

Send Jenkins build logs to Fortify Technical Support. Build log are located under,

Eg

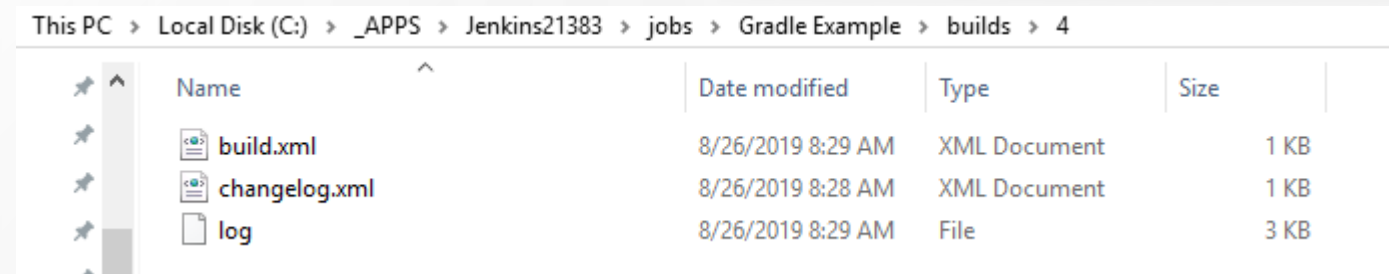
Path\Jenkins\jobs\



This PC > Local Disk (C:) > _APPS > Jenkins21383 > jobs > Gradle Example > builds >

Name	Date modified	Type
1	8/26/2019 8:13 AM	File folder
2	8/26/2019 8:15 AM	File folder
3	8/26/2019 8:23 AM	File folder
4	8/26/2019 8:29 AM	File folder

Console output can also be found in the \jobs directory under the same JOB ID



This PC > Local Disk (C:) > _APPS > Jenkins21383 > jobs > Gradle Example > builds > 4

Name	Date modified	Type	Size
build.xml	8/26/2019 8:29 AM	XML Document	1 KB
changelog.xml	8/26/2019 8:28 AM	XML Document	1 KB
log	8/26/2019 8:29 AM	File	3 KB

Additional Information

- Jenkins plugin documentation
[https://www.microfocus.com/documentation/fortify-jenkins-plugin/1910/Jenkins Plugin Help 19.1.0/index.htm](https://www.microfocus.com/documentation/fortify-jenkins-plugin/1910/Jenkins%20Plugin%20Help%2019.1.0/index.htm)
- Jenkins Plugin for Fortify SCA/SSC to automatically upload projects
<https://youtu.be/cjEwDmTsxII>
- Fortify Plugin
<https://wiki.jenkins.io/display/JENKINS/Fortify+Plugin>
- Pipeline-compatible steps
<https://jenkins.io/doc/pipeline/steps/fortify>

Questions

Thank you.

www.microfocus.com

