Micro Focus
Fortify Plugin for Bamboo

Software Version: 1.0

User Guide

Document Release Date: January 2018
Software Release Date: January 2018

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

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

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

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

Fortify Plugin for Bamboo

Use the Micro Focus Fortify Bamboo Plugin in your continuous integration builds to identify security issues in your source code with Micro Focus Fortify Static Code Analyzer. After the Fortify Static Code Analyzer analysis is complete, you can optionally upload the results to Fortify Software Security Center.

With the Fortify Plugin for Bamboo, you can integrate Fortify Static Code Analyzer with the following build tools:

- Gradle
- Maven
- MSBuild
- Visual Studio (devenv)

You can also scan your source code directly without a build tool.

The following table describes the workflow for setting up the Fortify Plugin for Bamboo.

Task	**For More Information...**
Add Fortify SCA to your Bamboo server capabilities.	"Preparing the Bamboo Server to Work with Fortify Static Code Analyzer" on page 7
Configure your plan to include the Fortify SCA task.	"Configuring the Fortify SCA Task" on page 8
Run your plan.	Atlassian Bamboo documentation
Review analysis results.	"Viewing the Results" on page 11

Software Requirements

The Micro Focus Fortify Bamboo Plugin works with the software packages listed in the following table. Your specific requirements depend on the programming language you are scanning and the build tools you are using. This table also provides information to help you prepare for the configuration of your Bamboo plan.

Software	**Version**	**Notes**
Atlassian Bamboo server	6.0 or later	
Fortify Static Code Analyzer	17.20 or later	To configure the Fortify SCA capability, you must have the path to the Fortify Static Code Analyzer executable (Windows: `sourceanalyzer.exe`, macOS and Linux: `sourceanalyzer`).

Software	**Version**	**Notes**
Fortify Software Security Center (Optional)	17.20 or later	To upload scan results to Fortify Software Security Center, make sure that you have the Fortify Software Security Center URL and either: • A Fortify Software Security Center username and password • A Fortify Software Security Center authentication token of type JenkinsToken The following is an example of the command to create an authentication token: `fortifyclient token -gettoken JenkinsToken -url <SSC_URL> -user <username> -password <password>`
Maven	3.x	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. You must install the Fortify Maven Plugin for the same user who is running Bamboo. For more information about build integration with the Fortify Maven Plugin, see the *HPE Security Fortify Static Code Analyzer User Guide*. **Note:** The Fortify Plugin for Bamboo uses the `sca` prefix for the translation with the Fortify Maven Plugin. For more information about a plugin prefix, see https://maven.apache.org/guides/introduction/introduction-to-plugin-prefix-mapping.html.
MSBuild	4.x, 12.0, 14.0, 15.0	
Visual Studio	2013, 2015, 2017	To scan .NET projects, Fortify recommends that the system have a full installation of Visual Studio and the Fortify Package for Visual Studio for your specific version of Visual Studio. To scan a project solution with devenv, configure a Bamboo executable server capability that specifies the path to the Visual Studio IDE folder (for example: `C:\Program Files (x86)\Microsoft Visual Studio\2017\Enterprise\Common7\IDE`).

Installing the Fortify Plugin for Bamboo

To install the Micro Focus Fortify Bamboo Plugin, you must have the Bamboo server installed on your system. You can download the Fortify Plugin for Bamboo from the Atlassian Marketplace (https://marketplace.atlassian.com) directly to Bamboo.

> **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 Plugin for Bamboo:

1. From the **Bamboo Administration** menu ⚙▾, select **Add-ons**.
2. Click **Find new add-ons**, and then search for **Fortify**.
3. Click **Install** to download and install the plugin.

Preparing the Bamboo Server to Work with Fortify Static Code Analyzer

Before you can use the Fortify SCA task to scan source code with Fortify Static Code Analyzer, you must add Bamboo server capabilities.

To add the **Fortify SCA** server capability, specify the settings described in the following table.

Field	Description
Capability type	Select **Executable**.
Type	Select **Fortify SCA**.
Executable label	Type a label such as `SCA <version>`, where `<version>` is the Fortify Static Code Analyzer version you are using.
Path	Type the path to the Fortify Static Code Analyzer executable (for example, on Windows the default installation path for version 17.20 is `C:\Program Files\HPE_Security\Fortify_SCA_and_Apps_17.20\bin\sourceanalyzer.exe`).

To integrate with Gradle, add the Fortify SCA Gradle executable capability. For integration with Maven or MSBuild, use the Bamboo-provided Maven and MSBuild executable capability types. To use devenv, use the Bamboo-provided Visual Studio executable capability.

See the *HPE Security Fortify Static Code Analyzer User Guide* for information about how to configure the Fortify SCA task with Gradle, Maven, or MSBuild.

Configuring the Fortify SCA Task

Add the Fortify Static Code Analyzer task to your plan and configure it to run the scan and, optionally, upload the results to Fortify Software Security Center. For more information about Fortify Static Code Analyzer command-line options, see the *HPE Security Fortify Static Code Analyzer User Guide*.

To add and configure the Fortify SCA task:

1. Add the Fortify SCA task to your plan.

   You can find he Fortify SCA task in the **Builder** task type section or you can search for `fortify`.
2. From the **Fortify SCA** list, select the Fortify Static Code Analyzer executable.

   The executable specifies the path to the Fortify Static Code Analyzer executable (Windows: `sourceanalyzer.exe`, macOS and Linux: `sourceanalyzer`). To create a new executable, click **Add new executable**. You might have multiple executables if you have more than one version of Fortify Static Code Analyzer installed.
3. In the **Build ID** box, type a unique identifier for the scan.
4. To specify the maximum heap memory or other JVM options, click **Advanced options**.

   > **Note:** Specify the maximum heap memory as an integer only. For example, to specify 48 GB, type `48000`.
5. To download Fortify security content before the scan, select the **Update Fortify Security Content** check box.

   To connect to the Fortify Rulepack update server with a proxy server, specify the proxy information.

   > **Note:** Use the following syntax for the **Proxy server URL**, where *`<protocol>`* is `http` or `https`, *`<address>`* is the Web address of the proxy server, and *`<port>`* is the port number assigned to the proxy server:
   >
   > *`<protocol>`*`://`*`<address>`*`:`*`<port>`*
6. To remove any temporary files from a previous scan for the specified build ID, select the **Run Fortify SCA Clean** check box.

   Fortify recommends that you run the clean phase before each translation unless, for example, you are translating several projects with the same build ID to perform one scan for all the projects and generate a single FPR file.
7. To run translation, select the **Run Fortify SCA Translation** check box, and then specify the translation settings.

   You might want to skip the translation if, for example, the security content has changed but the source code has not.

   > **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"`

a. Select whether you want to use the basic or advanced configuration.

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, if needed. See the *HPE Security Fortify Static Code Analyzer User Guide* for detailed information about the translation options.

Select **Basic** to be prompted to provide the typical information to scan Java or .NET code or to run a Maven 3, or Gradle build to perform the scan. The configuration fields dynamically change based on your selection. The following table describes each application type for the basic configuration.

Application Type	Description
Java	See the *HPE Security Fortify Static Code Analyzer User Guide* for more detailed information about the Java translation options.
.NET	i. Specify whether to perform a project solution or a source code scan. ii. To translate a solution: A. Select a build type: **Devenv** or **MSBuild**. B. From the **Executable** menu, select or configure a Visual Studio or an MSBuild executable (see "Preparing the Bamboo Server to Work with Fortify Static Code Analyzer" on page 7). C. Type the solution file name (or the path to the solution file). D. Specify any additional devenv or MSBuild options, depending on the executable you are using. iii. To translate source code: Specify all the Fortify Static Code Analyzer translation options, including source files. See the *HPE Security Fortify Static Code Analyzer User Guide* for detailed information the translation options.
Maven 3	i. Select or configure a Maven 3 executable (see "Preparing the Bamboo Server to Work with Fortify Static Code Analyzer" on page 7). ii. If you did not run the build previously, then in the **Maven options** box, type `package`. Otherwise, leave this box empty. **Note:** The translation log is located in the /target directory that is created when the “package” runs from Maven. Any log file location specified in the Fortify Plugin for Bamboo is ignored when the Fortify Maven Plugin performs the translation.
Gradle	i. Select a previously-configured Fortify SCA Gradle executable. ii. In the **Gradle tasks** box, type the Gradle tasks and options required for your project. The default value is `"assemble"`.
Other	This is very similar to the advanced configuration. You must manually provide all the Fortify Static Code Analyzer translation options.

b. To enable the debug or verbose options or to specify a custom location for the Fortify Static Code Analyzer log file, click **Advanced options**.

8. To run a scan, select the **Run Fortify SCA Scan** check box, and then specify the scan settings:

a. In the **Result file** box, type a name (and optionally the location) for the analysis results file (`<filename>.fpr`).

b. To use a custom issue template for the scan, type the path to the template file in the **Issue Template** box.

> **Note:** This only affects scans on the local machine. If you upload the FPR to Fortify Software Security Center, the results display uses the issue template assigned to the application version.

c. (Optional) Specify any additional analysis 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"`.

d. To enable the debug or verbose options or to specify a custom location for the Fortify Static Code Analyzer log file, click **Advanced options**.

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

a. To connect to the Fortify Software Security Center with a proxy server, select **Configure proxy server**, and then specify the proxy information.

> **Note:** Use the following syntax for the **Proxy server URL**: `<protocol>://<address>:<port>`

b. Provide your Fortify Software Security Center credentials.

You must provide either:

- a Fortify Software Security Center username and password
- an authentication token of type JenkinsToken

c. Specify an application name and version.

To create a new application version, select **Create new application version**. This creates a new application version if the application name and version specified does not currently exist on Fortify Software Security Center.

d. 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 *HPE Security Fortify Software Security Center User Guide* for a description of the search query syntax.

   e. In the **Timeout (ms)** box you can type the maximum amount of time in milliseconds to wait for a response from Fortify Software Security Center after the upload has completed. The default value is 300000 ms.

      The Fortify Plugin for Bamboo provides a timeout to avoid the possibility of impeding the build. To have the Fortify Plugin for Bamboo continue to poll Fortify Software Security Center until the processing is complete, leave the timeout box empty.

10. Click **Save**, enable the plan, and then click **Create**.

Viewing the Results

After you run the plan, check the logs to verify that the scan was successful. Review both the Bamboo build log and the Fortify Static Code Analyzer log file.

> **Note:** If you did not specify a custom location for the Fortify Static Code Analyzer log file in your Fortify SCA task, Fortify Static Code Analyzer saves the log file in `<userhome>\AppData\Local\Fortify\sca<version>\log\sca.log`, where `<version>` is the Fortify Static Code Analyzer version.

If you uploaded the results to Fortify Software Security Center, log in to Fortify Software Security Center and open the application version for which you saved your scan results. Otherwise, you can open the scan results (FPR file) in Fortify Audit Workbench, the Fortify Plugin for Eclipse, or the Fortify Package for Visual Studio.

Troubleshooting

Unable to connect to Fortify Software Security Center

- Make sure that your application name, version name, and SSC URL are correctly configured.
- If a proxy is required to connect to Fortify Software Security Center from your network, check the proxy configuration.
- If Fortify Software Security Center is configured to use HTTPS, make sure that the JDK keystore in the Fortify Static Code Analyzer installation is configured to accept the Fortify Software Security Center server certificate.

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 Plugin for Bamboo 1.0)

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!