Micro Focus
Fortify Jenkins Plugin

Software Version: 18.10

Installation and Usage Guide

Document Release Date: May 2018
Software Release Date: May 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

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
18.10	Updated: • Minor edits to incorporate branding changes • "Preparing Fortify Software Security Center to Work with the Jenkins Plugin" on page 7 - Updated the token type and the instructions for how to create an authentication token
17.20	Updated: • Minor edits Removed: • "Creating a Jenkins Token Type" - This is now provided automatically with Micro Focus Fortify Software Security Center
17.10	Updated: Release date and version number

Fortify Jenkins Plugin

The Fortify Jenkins Plugin (Jenkins Plugin) is used in conjunction with Micro Focus Fortify Software Security Center (Fortify Software Security Center), a collaborative system used to review and audit security analysis results. If you use a Micro Focus Fortify Static Code Analyzer plugin such as Maven to scan your source code after each build, the Jenkins plugin automatically uploads the Fortify Project Results (FPR) file to a Fortify Software Security Center server and enables you to view the details within Jenkins. It also provides metrics for each build and an overview of the results, without the need to connect to Fortify Software Security Center.

This document provides instructions on how to prepare Fortify Software Security Center to work with the Jenkins Plugin, and how to install, configure, and use the plugin. For information about Jenkins, see the Jenkins website (https://jenkins.io).

Installing the Jenkins Plugin

To install the 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 Jenkins Plugin:

1. From Jenkins, select **Manage Jenkins > Manage Plugins**.
2. On the **Plugin Manager** page, click the **Advanced** tab.
3. Under **Upload Plugin**, click **Choose File**, and then locate and select `Fortify_Jenkins_Plugin_<version>.hpi`.
4. Click **Upload**.
5. Restart Jenkins.

   If you started Jenkins locally, press **Ctrl**+**c** in the command-line window to restart it.

For more information about how to install Jenkins plugins, see the Jenkins Plugin site https://jenkins.io/doc/book/managing/plugins.

Verifying the Jenkins Plugin Installation

To verify that the Jenkins Plugin is installed:

1. Open a browser window and navigate to `http://<jenkins_server_url>: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 Jenkins Plugin

To prepare Micro Focus Fortify Software Security Center to work with the Jenkins Plugin, you need to have an authentication token of type CIToken created in Fortify Software Security Center. You will use this authentication token to configure the Jenkins Plugin.

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 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 of type CIToken using the fortifyclient utility:

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

   ```
   fortifyclient token -gettoken CIToken -url <ssc_url> -user <user_name>
   -daysToLive <number_of_days>
   ```

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

   where:

   - *<ssc_url>* includes both the port number and the context path `/ssc`. For example, `http://<hostname>>:<port>/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 Jenkins Plugin (see "Configuring the Jenkins Plugin" on the next page).

Configuring the Jenkins Plugin

To configure the Fortify Jenkins Plugin for use with Fortify Software Security Center:

1. Open a browser window and navigate to `http://<jenkins_server_url>:8080`.
2. From the Jenkins menu, select **Jenkins > Manage Jenkins > Configure System**.
3. In the **Fortify Assessment** section, do the following:
   a. In the **URL** box, type the Fortify Software Security Center server URL for which you configured the Jenkins token type.

      The correct format for the Fortify Software Security Center URL is: `http://<host_IP>:<port>/ssc`.
   b. In the **Authentication Token** box, type the authentication token generated for the Fortify Software Security Center server.

      See "Preparing Fortify Software Security Center to Work with the Jenkins Plugin" on the previous page.
4. Click **Advanced settings**, and then click **Test Connection**.

   The Jenkins Plugin populates the **Issue Template** list with available Fortify Software Security Center issue templates. 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.
5. From the **Issue Template** list, select the appropriate issue template for your projects.
6. Click **Save**.

Note: There is no need to specify a value in the **Issue breakdown page size** box at this time. You can always change this setting later. This setting controls the **Issue Breakdown** table view. The default is 50 issues per page.

Configuring the Build Step to use the Jenkins Plugin

To configure the build step to use the Jenkins Plugin:

1. From Jenkins, select the job to view or create a new job.
2. On the job page, click **Configure**.
3. On the configuration page that opens for the job, in the **Post-build Actions** section, select **Fortify Assessment**.
4. In the **Fortify Assessment** section, provide or change values for the properties and actions listed in the following table.

   Note: You can use job parameters in the **Fortify Assessment** properties in the following formats: `$param` and `${param}`.

Action or Property	Description
FPR Filename	The FPR name to publish (for example, `MyAudit.fpr`). If you do not specify a value, the Jenkins Plugin searches `"./**/*.fpr"` files in the workspace with the latest modified date.
FilterSet	Filter set to use when reading the FPR. If no value is specified, the default filter is used. Fortify Software Security Center has two filter sets: Security Auditor View and Quick View. Quick View is the default filter set. However, the issue template used to create the project determines the exact filter set configuration. The fail condition and the Normalized Vulnerability Score (NVS) calculation depend on the issues filtered by the filter set. For example, if a “Critical Exposure” filter is applied to the project issues (and no issues are found), then the fail condition determines that there is no reason to set this build to “unstable” and NVS is set to zero. The graph summary also shows zero.
Fail Condition	A build is considered unstable if the fail condition is met. For example, to get the unstable build where there is an SQL injection issue in the High folder, use the following search string for the fail condition: `[fortify priority order]:high category:SQL Injection` This search string syntax is the same as that used for the Fortify Software Security Center search and filter capabilities.
Application Name	Application name used when uploading FPR files to Fortify Software Security Center. Leave this field blank to disable the upload. Always use Application Name and Application Version together. To upload an FPR file to Fortify Software Security Center: • Specify both Application Name and Application Version. • Specify the Fortify Software Security Center URL and the authentication token (see "Configuring the Jenkins Plugin" on the previous page). **Note:** If an application with the specified name does not exist on Fortify Software Security Center, Fortify Software Security Center creates it for a successful build.
Application Version	Application version used when uploading to Fortify Software Security Center. Leave this field blank to disable the upload. Always specify Application Name and Application Version together.

Action or Property	Description
Upload Wait Time	To access this box, click **Auto Job Assignment**. Because the FPR upload to Fortify Software Security Center is asynchronous, the WebService function call is returned while Fortify Software Security Center is still processing the upload request. Therefore, the Jenkins Plugin waits for a specified number of minutes before it runs the NVS calculation. The valid values are 0-60.

5. Click **Save**.

Using the Jenkins Plugin with Continuous Builds

To use the Jenkins Plugin with continuous builds:

1. Place the FPR that resulted from a source code scan into the workspace directory for the project.

   On Windows systems, the default directory is `C:\Users\<username>\.jenkins\jobs\<project_name>\workspace`.

   Note: Configure your build procedure to do this automatically. You can specify the path to your FPR file with the **FPR Filename** setting on the **Job Configuration** page. For more information, see "Configuring the Build Step to use the Jenkins Plugin" on page 8.

2. From Jenkins, select **Build Now**.
3. To read progress messages from the Jenkins Plugin, in the **Build History** box, select the build link, and then, on the <*build_number*> page, select **Console Output**.
4. After the build completes successfully (after you see the `Finished: SUCCESS` message), return to the project page.

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

   ```
   NVS = ((CFPO * 10) + (HFPO * 5) + (MFPO * 1) + (LFPO * 0.1)) * 0.5 +
         ((P1 * 2) + (P2 * 4) + (P3 * 16) + (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

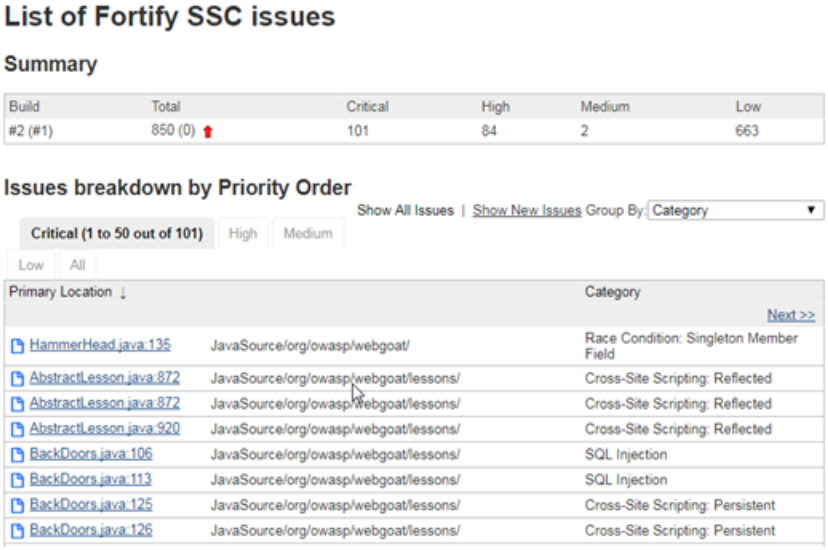
The total issues count is not very useful. For example, if Application A has 0 critical issues and 10 low issues, the total issue count is 10. If Application B has five critical issues and no low issues, the total issue count is 5. These values might mislead you to think that Application B is better than Application A, when it is not.

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

- Application A: NVS = 0*10 + 10*0.1 = 1
- Application B: NVS = 5*10 + 0*0.1 = 50

5. Click **Fortify Assessment** on the left.

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



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 too long, you might need to refresh the browser window (F5).

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.

Viewing Issues

To see only those issues that were introduced in the latest build of your code, click the **Show New Issues** link at the top of the table.

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, click **Advanced Settings**, and then change the value in the **Issue breakdown page size** 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 Installation and Usage Guide (Fortify Jenkins Plugin 18.10)

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!