opentext™

OpenText™ Fortify Bitbucket

Integration Guide

Document Release Date: September 2024

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Warranty

Trademark Notices

Bitbucket pipelines pipe: Fortify scan

The Fortify scan pipe for Bitbucket pipelines runs a Fortify on Demand scan or a Fortify ScanCentral SAST scan of your application for potential security vulnerabilities.

About Fortify

Fortify offers end-to-end application security solutions with the flexibility of on-premises and on-demand testing to scale and covers the entire software development lifecycle. With Fortify, find security issues early and fix them at the speed of DevSecOps.

About the Fortify scan pipe

The Fortify scan pipe enables you to easily integrate static application security testing (SAST) into your CI/CD pipelines and scan your application for potential security vulnerabilities. Additionally, you may configure the pipe to wait for scan completion and import the results into Code Insights, enabling full end-to-end security testing within the Bitbucket ecosystem.

The Fortify scan pipe is available at https://bitbucket.org/fortifysoftware/workspace/projects/BIT.

Known limitations

Currently, the Bitbucket Fortify pipe focuses on scanning Java applications. It does not include build tools for other languages, such as .NET, and might fail or produce inaccurate or incomplete scan results for languages that require build tool integration. For such languages, you might want to create a pipeline that does not use the Bitbucket Fortify pipe, but instead invokes the various Fortify tools directly. Consider the following tools:

- Fortify ScanCentral SAST Client (see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide* available at https://www.microfocus.com/documentation/fortify-static-code-analyzer-and-tools/)
- FoDUploader (see the FoDUploader documentation at https://github.com/fod-dev/fod-uploader-java?tab=readme-ov-file#current)
- fcli (see https://github.com/fortify/fcli/releases for the tool and https://fortify.github.io/fcli/ for the documentation)

Future versions of the Bitbucket Fortify pipe may provide better support for languages other than Java.

Prerequisites

To run Fortify on Demand scans, you must have an account on Fortify on Demand. To run Fortify ScanCentral SAST scans, you must have access to a Fortify Software Security Center and Fortify ScanCentral SAST environment.

If you are not already a Fortify customer, you may request a Free Trial.

Fortify on Demand scan

This section describes how to integrate a basic Fortify on Demand scan into a Bitbucket pipeline.

YAML definition snippet

To incorporate the Fortify scan pipe into your pipeline, you must add a YAML definition snippet to the script section of your `bitbucket-pipelines.yml` file. The following example shows a partial Bitbucket pipeline that runs a scan of a Maven-based application using Fortify on Demand and reports results back to Bitbucket.

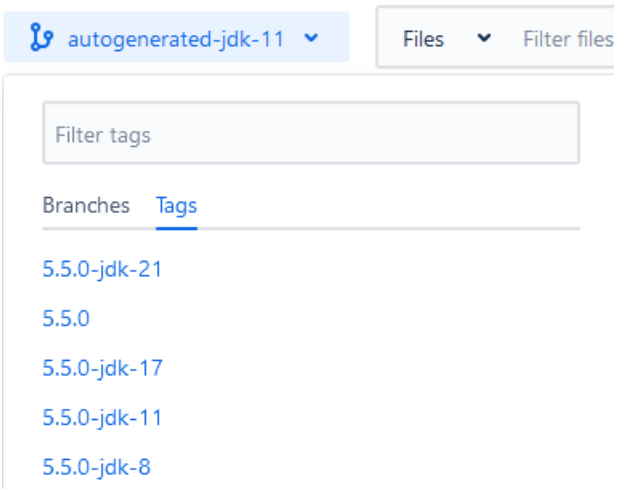
```
pipelines:
   default:
     - step:
         script:
         - pipe: fortifysoftware/fortify-scan:<version>
           variables:
             PACKAGE_OPTS: -bt mvn
             FOD_URL: $FOD_BASE_URL
             FOD_TENANT: $FOD_TENANT
             FOD_USER: $FOD_USER
             FOD_PASSWORD: $FOD_PASSWORD
             FOD_RELEASE_ID: $FOD_RELEASE_ID
             FOD_UPLOAD_OPTS: -ep 1
```

In this example, *<version>* is the version of the pipe that you want to run. More information about pipe version and input variables is available in the following sections.

Additionally, the snippet uses variable values that start with a `$` character, such as `$VARIABLE_NAME`. For information on how to define these variables using Bitbucket repository variables, see https://support.atlassian.com/bitbucket-cloud/docs/variables-and-secrets/.

Pipe versions

You can view available versions in the **Tags** list on the Bitbucket Fortify Pipe Source page, as shown below. If you are scanning a Java application, you should select a version that includes a suitable JDK version to build your application, such as `5.5.0-jdk-17`. For scanning non-Java applications, you can select a version without a `jdk` suffix, such as `5.5.0`, but consider the known limitations detailed in "Known limitations" on page 3.



Fortify on Demand variables

The following table describes the most used input variables for the Bitbucket Fortify pipe. For more details on these and other supported input variables, see the documentation for the pipe version that you are using in the Bitbucket repository at https://bitbucket.org/fortifysoftware/fortify-scan.

Important! Be sure to select the correct tag for the pipe version that you are using, as described in the previous section.

Variable	Description
`PACKAGE_OPTS`	Specifies packaging options that will be passed to the ScanCentral command. For example, you can use this option to specify '`-bt mvn`' or '`-bt gradle`'. This option does not have a default value and is required if `DO_PACKAGE` is set to `true`. For more information about packaging options, see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide* .
`FOD_URL`	Specifies the Fortify on Demand portal URL, such as

Variable	Description
	`https://ams.fortify.com`. This variable is required for running scans and exporting vulnerability data from Fortify on Demand.
`FOD_TENANT`	Specifies the Fortify on Demand tenant. This variable is required for running scans using Fortify on Demand and exporting vulnerability data from Fortify on Demand.
`FOD_USER`	Specifies the Fortify on Demand user name. This variable is required when connecting to Fortify on Demand with user credentials.
`FOD_PASSWORD`	Specifies the Fortify on Demand password. This variable is required when connecting to Fortify on Demand with user credentials.
`FOD_CLIENT_ID`	Specifies the Fortify on Demand client ID. This variable is required when connecting to Fortify on Demand with client/API credentials.
`FOD_CLIENT_SECRET`	Specifies the Fortify on Demand client secret. This variable is required when connecting to Fortify on Demand with client/API credentials.
`FOD_RELEASE_ID`	Specifies the Fortify on Demand release ID. This variable is required for running scans using Fortify on Demand and exporting vulnerability data from Fortify on Demand.
`FOD_NOTES`	Specifies optional scan notes to be passed to Fortify on Demand.
`FOD_UPLOAD_OPTS`	Specifies any additional options for FoDUploader. FoDUploader requires at least the '`-ep`' option to be passed. **Note:** Any relevant Fortify on Demand options listed above are automatically passed to FoDUploader. In addition, the following options are automatically passed to FoDUploader under certain conditions: • `-I 1` is passed if `DO_BLOCK` or `DO_EXPORT` is set to `true`. • `-apf` is passed if `DO_EXPORT` is set to `true`. For a list of available upload options, see the FoDUploader documentation at https://github.com/fod-dev/fod-uploader-java?tab=readme-ov-file#current.

Fortify ScanCentral SAST scan

This section describes how to integrate a basic Fortify ScanCentral SAST scan into a Bitbucket pipeline.

YAML definition snippet

To incorporate the Fortify scan pipe into your pipeline, you must add a YAML definition snippet to the script section of your `bitbucket-pipelines.yml` file. The following example shows a partial Bitbucket pipeline that runs a scan of a Maven-based application using Fortify ScanCentral SAST and reports results back to Bitbucket.

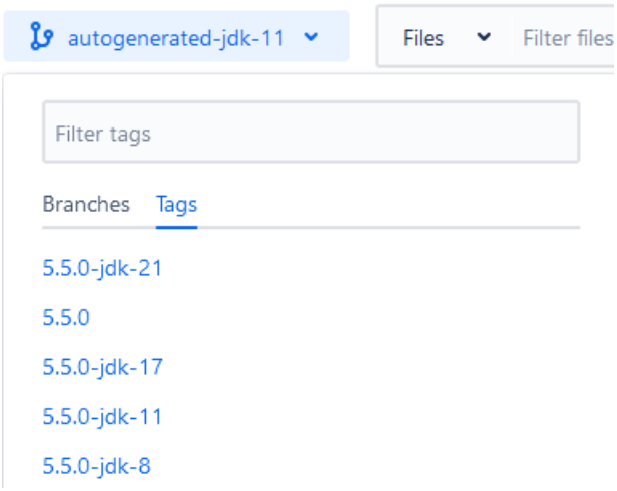
```
pipelines:
  default:
    - step:
        script:
          - pipe: fortifysoftware/fortify-scan:<version>
            variables:
              PACKAGE_OPTS: -bt mvn
              SCANCENTRAL_AUTH_TOKEN: CHANGEME321!
              SSC_URL: $SSC_BASE_URL
              SSC_CI_TOKEN: $SSC_CI_TOKEN
              SSC_VERSION_ID: $SSC_VERSION_ID
```

In this example, *<version>* is the version of the pipe that you want to run. More information about pipe version and input variables is available in the following sections.

Additionally, the snippet uses variable values that start with a `$` character, such as `$VARIABLE_NAME`. For information on how to define these variables using Bitbucket repository variables, see https://support.atlassian.com/bitbucket-cloud/docs/variables-and-secrets/.

Pipe versions

You can view available versions in the **Tags** list on the Bitbucket Fortify Pipe Source page, as shown below. If you are scanning a Java application, you should select a version that includes a suitable JDK version to build your application, such as `5.5.0-jdk-17`. For scanning non-Java applications, you can select a version without a `jdk` suffix, such as `5.5.0`, but consider the known limitations detailed in "Known limitations" on page 3.



Fortify ScanCentral SAST variables

The following table describes the most used input variables for the Bitbucket Fortify pipe. For more details on these and other supported input variables, see the documentation for the pipe version that you are using in the Bitbucket repository at https://bitbucket.org/fortifysoftware/fortify-scan.

Important! Be sure to select the correct tag for the pipe version that you are using, as described in the previous section.

Variable	Description
`PACKAGE_OPTS`	Specifies packaging options that will be passed to the ScanCentral command. For example, you can use this option to specify '`-bt mvn`' or '`-bt gradle`'. This option does not have a default value and is required if `DO_PACKAGE` is set to `true`. For more information about packaging options, see the *OpenText™ Fortify ScanCentral SAST Installation, Configuration, and Usage Guide* .
`SSC_URL`	Specifies the Fortify Software Security Center base URL, such as `https://my.ssc.host/ssc`. This setting is required for running scans using ScanCentral SAST and for exporting vulnerability data from Fortify Software Security Center.
`SSC_CI_TOKEN`	Specifies the Fortify Software Security Center CIToken used for authenticating with Fortify Software Security Center. This setting is required for running scans using ScanCentral SAST and for exporting vulnerability data from Fortify Software Security Center.

Variable	Description
SSC_VERSION_ID	Specifies the Fortify Software Security Center application version ID. This setting is required for running scans using ScanCentral SAST and for exporting vulnerability data from Fortify Software Security Center.
SCANCENTRAL_AUTH_TOKEN	Specifies the client auth token to be used for accessing the ScanCentral Controller.

Support and Documentation

For support on issues related to integration with Fortify products, visit the Support website at https://www.microfocus.com/support.

For more information, you can access the latest versions of Fortify product documentation from the Product Documentation website at https://www.microfocus.com/support/documentation.