




BLACKDUCK

Installing, Configuring, and
Using the Hub Plugin for
Bamboo

Version 3.0.1



This edition of the *Installing, Configuring, and Using the Hub Plugin for Bamboo* refers to version 3.0.1 of the Black Duck Hub Plugin for Bamboo.

This document created or updated on Wednesday, February 08, 2017.

Please send your comments and suggestions to:

Black Duck Software, Incorporated
800 District Avenue
Suite 221
Burlington, MA 01803 USA.

Copyright © 2017 by **Black Duck Software, Inc.**

All rights reserved. All use of this documentation is subject to the license agreement between Black Duck Software, Inc. and the licensee. No part of the contents of this document may be reproduced or transmitted in any form or by any means without the prior written permission of Black Duck Software, Inc.

Black Duck, Know Your Code, and the Black Duck logo are registered trademarks of Black Duck Software, Inc. in the United States and other jurisdictions. Black Duck Code Center, Black Duck Code Sight, Black Duck Export, Black Duck Hub, Black Duck Protex , and Black Duck Suite are trademarks of Black Duck Software, Inc. All other trademarks or registered trademarks are the sole property of their respective owners.

Chapter 1: Hub Bamboo Plugin Overview	4
1.1 Supported Archive Types	4
1.2 Hub Bamboo Plugin Requirements	5
Chapter 2: Installation Overview	6
2.1 Installation Prerequisites	6
2.2 Downloading and Installing the Hub Bamboo Plugin	6
2.3 Updating the Hub Bamboo plugin	6
Chapter 3: Using the Hub Bamboo Plugin	7
3.1 Scanning Within the Workspace	7
3.2 Directory Exclusion Patterns	8
3.3 Code Locations	9
3.4 Cleaning Up Logs on Successful Scans	10
3.5 Dry Run Scanning	11
3.6 Report Configuration	11
3.7 Showing the Black Duck Hub Risk Report in Bamboo	12
3.8 Configuring Hub Risk Reports	12
3.9 Generating Reports	13
3.10 Viewing Reports in Bamboo	13
3.11 Hub Failure Conditions	14
3.12 Troubleshooting the Hub Bamboo Plugin	15
Chapter 4: Hub Bamboo Plugin Release Notes	17
4.1 Hub Bamboo Known Issues	18
Chapter 5: Black Duck Support	19
5.1 Training	19
5.2 Services	20

Chapter 1: Hub Bamboo Plugin Overview

Black Duck Hub is a new risk management tool designed to help you manage the logistics of using open source software in your organization.

The Black Duck Hub Scanner is the software component scanning functionality in Black Duck Hub that provides an automated way to determine the set of open source software (OSS) components that make up a software archive. The Hub Scanner is designed to help organizations manage their use of open source binaries by identifying and cataloging OSS components to provide additional metadata such as license, vulnerability, and OSS project health for those components.

Bamboo is an open source continuous integration tool that monitors executions of repeated jobs, such as building a software project or cron jobs. Bamboo focuses on building and testing software projects continuously and monitoring execution of externally run jobs.

As a Hub and Bamboo user, the Hub Bamboo plugin enables you to:

- Run a component scan in a Bamboo job:
 - Scan multiple targets within the job workspace.
 - Define the component scan command line interface (CLI) as a tool.
 - Create projects and releases in Black Duck Hub through the Bamboo job.
- After a scan is complete, the results are available on the Hub server.

Using the Hub Bamboo Plugin together with the Hub Scanner lets you use Bamboo to automatically create Hub projects from your Bamboo projects.

1.1 Supported Archive Types

The Hub Scanner can scan archive files as well as a directory of files. The following archive file types can be processed by the Hub Scanner:

The Black Duck Component Scanning can extract the following archive types:

- AR
- ARJ
- CPIO
- DUMP
- TAR
- RPM
- ZIP
- 7z

Archives may optionally be compressed using any of the following compression algorithms:

- Bzip2
- Gzip
- Pack200
- XZ
- LZMA
- Snappy
- Z (compress)
- DEFLATE

Note: If you attempt to scan an individual archive file that is not a supported type, the Hub Scanner finds no matches.

1.2 Hub Bamboo Plugin Requirements

Software Requirements

The installation instructions in this document assume that you have the following installed and configured on your system:

- Black Duck Hub 2.4 or higher
- Bamboo versions 5.10.0 or higher
- Java SE 7

Note: The Hub Scanner CLI client requires Java Runtime Environment (JRE) version 1.8.0_40 or later to be installed on the computer where it is run. For Hub versions 3.0 and higher, this is not required.

Note: For the complete listing of operating systems supported by Black Duck, refer to the *Black Duck Hardware Software Specifications*.

- Maven 3
- Microsoft Build version 11 or 12. Note that Visual Studio 2012 installs Microsoft Build 11, and Visual Studio 2013 installs Microsoft Build 12.
- Microsoft .NET Framework version 4.5

The Bamboo plugin is supported on the same operating systems and browsers as Black Duck Hub.

Network Requirements

The Hub Bamboo plugin requires internet connectivity. The machine that hosts your Bamboo server must be able to connect to the Hub server.

2.1 Installation Prerequisites

Before you install the Hub Bamboo plugin, ensure that:

- Your Bamboo instance is up-to-date and fully patched.
- You know the host name and port for the Hub server.
- You have a user account with administrator privileges on the Hub system that you can use for the integration.
- You have connectivity to the internet. The machine that hosts your Bamboo server must be able to connect to the Hub server.

2.2 Downloading and Installing the Hub Bamboo Plugin

Download the Bamboo plugin as described, then install the plugin using Bamboo.

Note: You must have administrator rights to install the plugin.

* To download the Hub Bamboo plugin:

1. Navigate to <https://github.com/blackducksoftware/hub-bamboo>.
2. Click the Gear icon and select **Add-ons**. The **Add-ons** page opens.
3. At the **Add-ons** page, click **Upload Add-on**.
4. To upload the add-on, you can either point to the downloaded installer on your local hard drive, or you can enter the URL to the GitHub release page (from step 1).
5. Click **Upload**. The **Download and installing** status message displays. When complete, a confirmation displays, stating that the download and installation was successful.
6. Verify that the Black Duck plugin (**Black Duck Hub Plugin for Bamboo**) displays in the Atlassian user-installed add-ons list. The plugin displays grayed-out if it is disabled.

2.3 Updating the Hub Bamboo plugin

You can update the Hub Bamboo plugin as new versions are released. The update procedure is the same as the installation procedure. For the installation procedure, refer to [Downloading and Installing the Hub Bamboo Plugin](#) on page 6.

Chapter 3: Using the Hub Bamboo Plugin

* To use the Bamboo plugin to scan a job:

1. In Bamboo, go to the configured Job.
2. Click the **Run** drop-down selector, and select **Run Plan** to execute the build.

You can view the messages output from the **Bamboo Console Output** screen. In Bamboo, click the build, then click the **Logs** tab.

You can also view the logs from the Hub Scanner in the following directory:

```
{WORKSPACE}/HubScanLogs/{BUILD_NUMBER}/log
```

You can view the results of the Hub Scanner on the Hub server. In Hub, click the expanding menu icon, then click **Component Scans**.

- To map a scan to a project, click **Map to Project**.
- To view the BOM, click **Bill of Materials**.
- To view the mapped project, click the project name.
- To view the mapped release, click the release name.

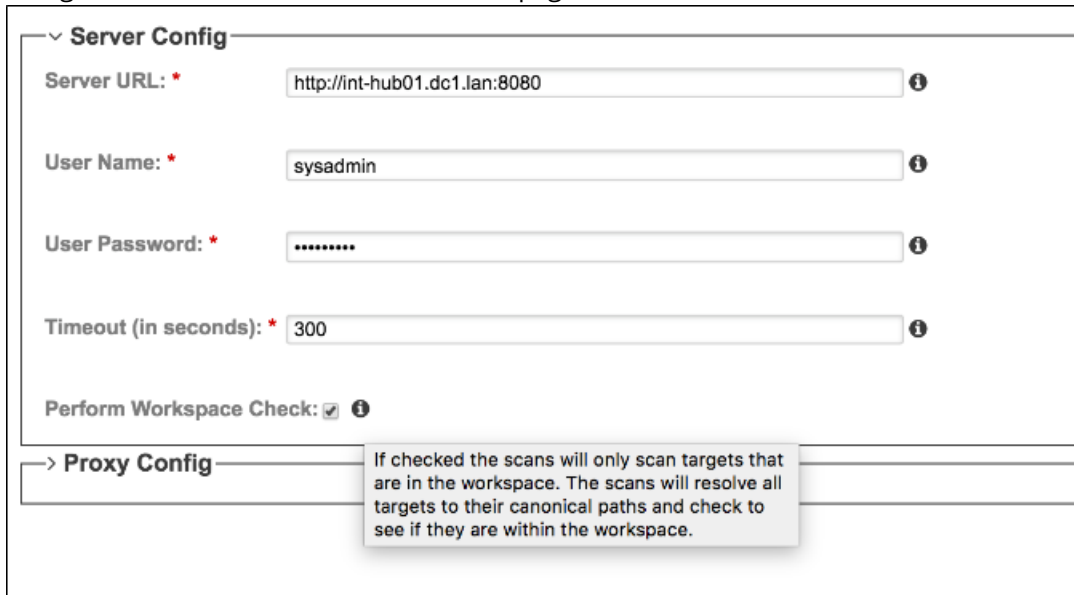
Alternatively, you can also view the logs from the BlackDuck scans in the directory `{SCAN_HOME}/lib/log`.

3.1 Scanning Within the Workspace

As of Hub Bamboo plugin versions 3.0.0 and higher, you can globally configure your workspace scanning option. This option enables you to scan projects outside your workspace. No longer are you required to move workspaces; you can simply point to the other workspaces and execute the scan. The **Perform Workspace Check** setting is global; you cannot turn it on or off based on specific scans.

* To configure workspace scanning:

1. Navigate to the **Bamboo administration** page.



The screenshot shows the 'Server Config' panel in the Bamboo administration interface. It contains the following fields:

- Server URL:** (with an information icon)
- User Name:** (with an information icon)
- User Password:** (with an information icon)
- Timeout (in seconds):** (with an information icon)
- Perform Workspace Check:** ☒ (with an information icon)

Below the 'Perform Workspace Check' checkbox is a section for 'Proxy Config'. A tooltip is displayed over this section with the text: 'If checked the scans will only scan targets that are in the workspace. The scans will resolve all targets to their canonical paths and check to see if they are within the workspace.'

2. At the bottom of the **Server Config** panel on the **Bamboo administration** page, set the **Perform Workspace Check** option:
 - a. *On* (checked) means that only targets that are in the workspace are scanned. The scans resolve all targets to their canonical paths, and verify that they are within the workspace.
 - b. *Off* (unchecked) means that workspaces outside your workspace are scanned.
3. Click **Save**.

Canonical paths are specified because links within workspaces that point to external workspaces are not allowed. If this is attempted, the build fails with the error *Cannot scan outside workspace*. If **Perform Workspace Check** is turned off, external workspaces are scanned without error or build failures, as long as Bamboo has access permissions to read those targets.

Important: Turning **Perform Workspace Check** off can cause security issues, as the scan is then allowed to scan areas to which the user does not have rights.

Note: If you have the plugins for *Hub Bamboo* and *Hub Atlassian Config* installed, a message displays at the top of the **Bamboo administration** page which states *You have the Hub Atlassian Config installed, please un-install that plugin to reduce confusion*. This is because workspace settings were previously only accessible in the *Hub Atlassian Config* plugin; this functionality is now moved into the *Hub Bamboo* plugin, thus making the *Hub Atlassian Config* plugin no longer required.

3.2 Directory Exclusion Patterns

Hub Bamboo plugin versions 3.0.0 and higher feature Directory Exclusion Pattern functionality. This

enables you to specify sub-directories to exclude from scans.

Directory Exclusion Pattern syntax rules:

The Directory Exclusion Pattern functionality follows the GIT *ignore* pattern. The syntax is:

```
/*name_of_sub-directory_to_exclude/
```

- Leading and trailing forward slashes are required; in other words, the exclusion pattern must start with **/** and end with **/**.
- Directory names cannot contain double asterisks (**).

Using Directory Exclusion Pattern ignores all contents of the specified sub-directory during scans. Additionally, you can specify full paths; for example, the command `/*Parent/Child1/Child2/` excludes the *Child2* sub-directory from the scan. Directory Exclusion Pattern also performs validation.

* To add directory exclusion patterns:

1. Navigate to the **Black Duck Hub Scan Task configuration** page.
2. On the **Black Duck Hub Scan Task configuration** page in the **Directory Exclusion Pattern** text box, type the directory exclusion pattern using the syntax rules previously described. To add multiple excluded directories, type one excluded pattern per line.
3. Click **Save**.

Note: Directory Exclusion Pattern only excludes sub-directories inside the scan targets. It cannot exclude archives or directories and contents inside an archive.

3.3 Code Locations

Hub Bamboo plugin versions 3.0.0 and higher features a new **Code Location** field on the configuration page. Using the code location functionality can make your continuous integration build process smoother and easier, and allows for multiple users scanning the same code base. Using the **Code Location** field is optional.

Black Duck Hub Integration

Project Name: JR Test
This Project exists on the Hub Server : http://int-hub01.dc1.lan:8080

Project Version: 2.0
This Version exists in the Project : JR Test

☐ Generate Black Duck Risk Report

Maximum time to wait for BOM update (in minutes): 5

Scan Memory Allocation: 4096

Code Location Name:
 This will change the name of the Code Location that is created by this scan.
 An example of a consistent Code Location across nodes and builds would be `${JENKINS_URL}-${JOB_NAME}`
 (from [Black Duck Hub Plugin for Jenkins](#))

☐ Dry Run

☐ Cleanup logs on successful scan

The **Code Location** field is hidden by default; click **Advanced** to display this field. The command line interface uses the "- -" (dash dash) name option. The **Code Location** field automatically adds the "- -" value. The **Code Location** field:

- Allows you to supply the name of your code location.
- Creates the command for you.
- Automatically adds it to the build action.

Continuous integration build processes have slaves or agents. The **Code Location** field automatically creates a local workspace on the machine issuing the commands. However, the target name is different, and is *host name* followed by *path*.

If two users are scanning the same code on continuous integration systems, the code location functionality automatically updates the Bill of Materials when more than one instance of the scan occurs, as long as both code locations match.

The **Code Location** field accepts Jenkins variable syntax. One example of a consistent code location across nodes and builds is `${BAMBOO_URL}-${JOB_NAME}`. If you are using Jenkins continuous integration, you must use Jenkins variable syntax.

3.4 Cleaning Up Logs on Successful Scans

Hub Bamboo plugin versions 3.0.0 and higher provide functionality to automatically remove log files for successful scans. This functionality can save substantial hard drive space, and improve performance.

* To automatically delete log files on successful scans:

1. On the configuration page, click **Advanced**.
2. In the advanced options, click the checkbox for **Cleanup logs on successful scan**.

If the scan has no errors, then no logs are generated when this field is selected. Note that the default option is unchecked.

3.5 Dry Run Scanning

As of Hub Bamboo plugin versions 3.0.0 and higher, you now have the option to execute dry run scans. The **Dry Run** option allows you to perform scans without uploading the scan results to the server. It creates a JSON file of the scan results within the workspace, which is located in `HubScanLogs/{BUILD_NUMBER}/data/`.

The **Dry Run** option is a checkbox, located in the **Black Duck Hub Scan Task configuration** page, below the **Scan Memory Allocation** field.

Because **Dry Run** does not upload scan results to the server:

- Project and version are not required, and are ignored if they are provided.
- No report is generated since the scan results are never sent to the Hub.
- Failure conditions are not run since the scan results are never sent to the Hub.

If you configure the scan to be a dry run, the following message appears in the logs if you have added the failure conditions: *Will not run the Failure conditions because this was a dry run scan.*

3.6 Report Configuration

You can configure Bamboo to generate Hub reports.

* To configure Bamboo for Hub reports:

1. In Bamboo, navigate to **Configure Job**.
2. In **Configure Job**, navigate to **Actions > Configure Plan > Job > Black Duck Hub Scan Task**.

Note: There is a section named **Black Duck Scan Task**. The plugin automatically configures this to automatically install the CLI into the Bamboo **Tools** directory. You no longer need to download the CLI and configure the location.

3. Click **Save**.
4. Return to the **Dashboard**.
5. Click a job.
 - a. Click **Configure**.
 1. If multiple JDKs are defined, select the one to use from the JDK drop down list near the

top of the configuration.

2. Type the **Project Name**.
3. Type the **Project Version**. Leave the **Project Name** and **Project Version** fields empty if you do not want the scans to be mapped to a particular Version. The resulting scans for the specified scan targets are automatically mapped to the specified project version.
4. If creating a new version, select the phase and distribution types. The phase and distribution can only be used to create new versions. The phase and distribution of existing versions are not updated.
5. If the project or version does not exist, you can create the project or version by clicking **Create Project/Version**.
6. If the project or version contains a variable, they can not be created from the job configuration.
7. If the project or version does not exist, they are created during the build.

3.7 Showing the Black Duck Hub Risk Report in Bamboo

You can display the Black Duck Hub risk report within Bamboo.

✳ To show the Hub risk report in Bamboo:

1. In **Task Configuration**, select **Generate Black Duck Risk Report**.
2. Specify the maximum amount of time to wait for the report. If the Hub BOM for the specified version is not updated with the information from the scan within the specified time, a timeout is forced. The build is pass or fail. The build fails if the timeout occurs.
3. Enter the amount of memory to allocate to the Black Duck Scan in megabytes. The default is 256MB.
4. Enter the target to scan.
5. To define more targets, add more scan targets by entering them on a new line in the text area. If you do not specify a target, the entire workspace is scanned.
6. Click **Save**.

3.8 Configuring Hub Risk Reports

To generate Hub risk reports within Bamboo, you must perform the following configuration.

✳ To show the Hub risk report in Bamboo:

1. Navigate to the **Configuration** page.
2. Under **Task Configuration**, select **Generate Black Duck Risk Report**

- Specify the maximum amount of time to wait for the report. If the Hub BOM for the specified version is not updated with the information from the scan within the specified time, a timeout is forced. The build is pass or fail. The build fails if the timeout occurs.
- Enter the amount of memory to allocate to the Black Duck scan in megabytes. The default is 256MB.
- Enter the target to scan.
- To define more targets, add more scan targets by entering them on a new line in the text area. If you do not specify a target, the entire workspace is scanned. If you do not specify a target, the entire workspace is scanned.
- Click **Save**.

3.9 Generating Reports

* To generate reports in Hub Bamboo:

- Go to the configured job.
- Click the **Run** drop-down selector and select **Run Plan**. The BlackDuck scans messages display in the console output of the build.
- If you selected **Generate Black Duck Risk Report**:
 - Click the build; the **Black Duck Risk Report** displays in the sidebar.
 - Click **Black Duck Risk Report** to open a page with a summary of the Black Duck Risk Report for the specified version. The results display for the BlackDuck Scans in the Hub server.

Job: Default Job was successful

Job Summary | Tests | Commits | Artifacts | Logs | Hub Risk Report | Metadata

Black Duck Risk Report

PSTestApp ▶ 1.0 See more detail...

Phase: In Planning | Distribution: External

Security Risk		License Risk		Operational Risk	
High	0	High	2	High	2
Medium	0	Medium	0	Medium	0
Low	0	Low	0	Low	3
None	8	None	6	None	3

BOM Entries: 8

Component	Version	License	H	M	L	Lic R	Opt R
Aspectacular	Release_2.1.8.0	MIT License	0	0	0	-	L
DynamicRestProxy	1.1.0	Apache License 2.0	0	0	0	-	L
golismero	0.5.2	GNU General Public License v2.0 or later	0	0	0	H	H
iSynaptic.Core.CodeGeneration	v0.2.0.0	MIT License	0	0	0	-	-
Kotlin	build-1.0.0	Apache License 2.0	0	0	0	-	L
maven-reference-en	mvnref-book-parent-0.2.1	Unknown License	0	0	0	H	H
Microsoft HTTP Client Libraries	2.2.29	Microsoft EULA Software	0	0	0	-	-
promises-book	1.4.1	MIT License	0	0	0	-	-

3.10 Viewing Reports in Bamboo

You can view Black Duck Hub Risk reports in Bamboo.

✱ **To view Black Duck Hub Risk reports:**

1. Click the **Logs** tab.
2. Under **Job**, click the **Default Job**. The **Default Job** shows the complete output of all log messages occurring during the build. The configuration information also displays in the log file. Note that the log displays in real-time as the scan is running. Error messages in log display in red. Examine the **Hub Scan Task Result** log entry to see if the Hub scan task was a success or failure. A fail code of zero is correct for CLI. If the CLI return code is anything other than zero, it fails the build.
3. Click the **Hub Risk Report** tab if *Generate Risk Report* is specified in the configuration. The report displays in Bamboo.

3.11 Hub Failure Conditions

Black Duck Hub Failure Conditions: This functionality is new for Hub version 3.0.0, and checks the BOM to verify if any components are in violation of a policy. If so, it fails the build. This function is not available if the server you defined does not support policies.

✱ **To configure failure conditions:**

1. Go to **Job Configuration > Task Configuration**.
2. Select **Fail the Build for Hub Policy violations**.

Tasks

A task is a piece of work that is being executed as part of the build. The execution of a script, a shell command, an Ant Task or a Maven goal are only few examples of Tasks. [Learn more about tasks.](#)

You can use [runtime](#), [plan](#) and [global variables](#) to parameterize your tasks.

Black Duck Hub Scan Task configuration

Task description

☐ Disable this task

Project Name:

Version:

Phase:

Distribution:

☐ Generate Black Duck Risk Report:

☒ Fail Build on Black Duck Hub Policy Violations

Maximum time to wait for report (in minutes):

Hub Scan Memory (in MBs):*

Scan Targets:

* To use failure condition functionality once configured:

1. Click the **Run** drop-down selector, and select **Run Plan**.
2. The build is set to *Failure* if the overall BOM status is *In Violation*, meaning there are components in violation of a defined policy.

Things to keep in mind when using failure conditions:

- The Black Duck Hub failure conditions can only be configured if the Black Duck Hub Integration is also configured.
- The Black Duck Hub failure conditions must be configured after the Black Duck Hub Integration step in the job configuration. Post-build actions run in the order they are configured.
- If the Black Duck Hub failure conditions are configured, and then the global configuration changes to use a Hub server that does not support policies, an error displays. If a build is run, it is set to **Failed**.

3.12 Troubleshooting the Hub Bamboo Plugin

If an error message is generated that states *During development and testing the following errors were encountered*, use the following solutions:

- If you try to use Java 6 instead of Java 7, instead of getting an *Unsupported major:minor version error* message, the plugin sometimes throws a false *java.lang.OutOfMemoryError: Java heap space* message instead.
- If you get a message that reads *Service Unavailable*, either the Hub server can't be reached, or the request to the server is invalid. Contact your Hub server administrator.
- If you get a *Precondition failed* error message, then the request to the server is invalid. Verify that your global configuration is correct, and verify that the job configuration is correct. If you are still getting this message after you have checked your configuration, contact your Black Duck technical account manager.
- If you get a *Not Found (404) - Not Found* error message, then the request to the server is invalid. Contact your Black Duck technical account manager.

Tip: After major releases of Hub, check for updated versions of your Black Duck plugins. Changes to the APIs, schema, and SDK versions may require updated versions of the integration plugins.

- The plugin automatically attempts to create the project. If you try to use the Hub Bamboo integration, and you configure a job with a project and version, and that project already exists but the current Hub user is not assigned to it, then the following errors display:
 - If you run the build, the following displays:

Status : 412

Response : {"errorMessage":"project name already exists","arguments":{"fieldName":"name"},"errors":[{"errorMessage":"project name already exists","arguments":{"fieldName":"name"},"errorCode":{"central.constraint_violation.project_name_duplicate_not_allowed}}],"errorCode":{"central.constraint_violation.project_name_duplicate_not_allowed}}"

Problem creating the project.

Assigning the current user to the existing project with this name resolves the issue.

Chapter 4: Hub Bamboo Plugin Release Notes

Changes in Release 3.0.1

- Addressed an issue wherein the Risk report was not rendering properly due to a missing path error.

Changes in Release 3.0.0

- Users can now globally configure scanning within workspaces.
- Added the option to automatically remove log files for successful scans.
- Added the option to exclude specific directories during scans.
- Added support for code location configuration.
- Added the option for dry run scanning.
- Atlassian configuration is no longer a prerequisite for Hub Bamboo installation.

Changes in Release 2.0.1

- Proxy configuration settings are no longer cached.
- Addressed a browser compatibility issue with Internet Explorer and Firefox wherein sorting the risk report table was not working as expected.
- Addressed an issue wherein the CLI required an environment variable.
- The BDIO environment variable is now being correctly passed into the scan process.
- The Hub Risk Report now shows component policy violations.
- Addressed an issue wherein the *In Development* phase was not always working as expected.
- Addressed an issue wherein running a build in Bamboo with an overridden policy violation in the Hub would fail the build.
- The installation process now preserves the certificates with the bundled JRE from the Hub command line interface (CLI).

Changes in Release 2.0.0

- Added support for Bamboo versions 5.10.0 and higher.

Changes in Release 1.0.0

- Addressed an issue regarding the installation and configuration of the plugin.
- Addressed the `NullPointerException` when installing the Hub Scan CLI during the execution of the Black Duck Hub *Scan Task*.

Changes in Release 0.1.0

- Black Duck Hub Admin configuration is now located in the **Add-ons** section of the Bamboo server.
- Black Duck Hub Admin supports configuring the Hub URL, user name, and password.

- Added the Black Duck Hub **Scan Task** to configure scanning a project and uploading data to the Black Duck Hub.
- Supports build failure on Black Duck Hub policy violations.
- Requires the Atlassian Plugin SDK version 5.0.13 for development purposes.

4.1 Hub Bamboo Known Issues

The following are known issues for the Hub Bamboo plugin.

Known Issues in Release 1.0.0

- If more than one process tries to perform the CLI install at the same time to the same directory (on the same machine), then the processes collide with each other and start deleting files while another creates them.
 - Workaround: When a process finds that the currently installed CLI must be updated (downloaded for the first time or to change the current files), then it should create a `.locked` file (or a similar and appropriate file name), then perform the update, and remove the `.locked` file when the update is complete. If another process starts to perform the install, it should first check for the `.locked` file, if it exists, then it should wait until the `.locked` file is deleted before performing its check.

Chapter 5: Black Duck Support

If you have questions or find issues, contact Black Duck Software.

For the latest in web-based support, access the Black Duck Software Customer Support Web Site:
<https://www.blackducksoftware.com/support/contact-support>

To access a range of informational resources, services and support, as well as access to Black Duck experts, visit the Black Duck Customer Success portal at:
<https://www2.blackducksoftware.com/support/customer-success>

You can also contact Black Duck Support in the following ways:

- **Email:** support@blackducksoftware.com
- **Phone:** +1 781.891.5100, ext. 5
- **Fax:** +1 781.891.5145
- **Standard working hours:** Monday through Friday 8:00 AM to 8:00 PM EST

Note: Customers on the **Enhanced Customer Support Plan** are able to contact customer support 24 hours a day, 7 days a week to obtain Tier 1 support.

If you are reporting an issue, please include the following information to help us investigate your issue:

- Name and version of the plugin.
- Black Duck product name and version number.
- Third-party integrated product and version; for example, Artifactory, Eclipse, Jenkins, Maven, and others. For Black Duck Hub, only Jenkins, TeamCity, and Bamboo is supported.
- Java version.
- Black Duck KnowledgeBase version, where applicable.
- Operating system and version.
- Source control management system and version.
- If possible, the log files, configuration files, and Project Object Model (POM) XML files.

5.1 Training

Black Duck training courses are available for purchase. Learn more at
<https://www.blackducksoftware.com/services/training>.

View the full catalog of our online offerings: <https://www.blackducksoftware.com/academy-catalog>.

When you are ready to learn, you can log in or sign up for an account:
<https://www.blackducksoftware.com/academy>.

5.2 Services

If you would like someone to perform Black Duck Software tasks for you, please contact the Black Duck Services group. They offer a full range of services, from planning, to implementation, to analysis. They also offer a variety of training options on all Black Duck products. Refer to <https://www.blackducksoftware.com/services/> for more information.