BLACKDUCK

BY SYNOPSYS®

Release Notes

Version 5.0.0

This edition of the *Release Notes* refers to version 5.0.0 of Black Duck.

This document created or updated on Friday, September 21, 2018.

Please send your comments and suggestions to:

Black Duck Software, Incorporated
800 District Avenue, Suite 201
Burlington, MA 01803-5061 USA

Contents

Black Duck Security Advisories (BDSA) 6

Ability to View Components with Cryptography 6

Assess to REST APIs through an API Key 6

New Scan Service 7

New Features in Version 4.3.1 7

End User License Agreement 7

New Features in Version 4.2.0 7

License Management 7

New License Manager Role 7

OpenShift Support 7

Ability to Compare BOMs 7

Enhanced Vulnerability Data 7

Ability to Configure Black Duck Session Timeout Value 7

New Feature in Version 4.1.1 8

Support for IDP Metadata XML File for SAML 8

New Features in Version 4.1.0 8

Kubernetes Support 8

New Features in Version 4.0.0 8

Summary Dashboard 8

External PostgreSQL Database 8

Remediation Guidance - BETA 8

Cross-site Request Forgeries 8

SAML for Single Sign-On Support 8

Web Server Configuration Settings 8

Default User Landing Page 8

New Features in Version 3.7.0 9

New Black Duck Docker Architecture 9

Issue Tracker 9

Chapter 3: Changed Features **10**

Changed Features in 5.0.0 10

Custom Component Management Enhancements 10

Operational Risk Enhancements 10

Local Logout Supported in SSO 10

API Enhancements 10

BOM Modifications Icon 11

Change in License Management Status 11

Japanese Language 11

Changed Features in 4.8.2 11

Changed Features in 4.8.1 11

Changed Features in 4.8.0 11

New Phase for Project Versions 11

Black Duck documentation

The documentation for Black Duck consists of online help and these documents:

Title	File	Description
Release Notes	release_notes.pdf	Contains information about the new and improved features, resolved issues, and known issues in the current and previous releases.
Installing Black Duck using Docker Compose	install_compose.pdf	Contains information about installing and upgrading Black Duck using Docker Compose.
Installing Black Duck using Docker Swarm	install_swarm.pdf	Contains information about installing and upgrading Black Duck using Docker Swarm.
Installing Black Duck using Kubernetes	install_kubernetes.pdf	Contains information about installing and upgrading Black Duck using Kubernetes.
Installing Black Duck using OpenShift	install_openshift.pdf	Contains information about installing and upgrading Black Duck using OpenShift.
Getting Started	getting_started.pdf	Provides first-time users with information on using Black Duck.
Scanning Best Practices	scanning_best_practices.pdf	Provides best practices for scanning.
Getting Started with the SDK	getting_started_sdk.pdf	Contains overview information and a sample use case.

Title	File	Description
Report Database	report_db.pdf	Contains information on using the report database.
User Guide	user_guide.pdf	Contains information on using Black Duck's UI.

Black Duck integration documentation can be found on Confluence.

Training

Synopsys Software Integrity, Customer Education (SIG Edu) is a one-stop resource for all your Black Duck education needs. It provides you with 24x7 access to online training courses and how-to videos.

New videos and courses are added monthly.

At Synopsys Software Integrity, Customer Education (SIG Edu), you can:

- Learn at your own pace.
- Review courses as often as you wish.
- Take assessments to test your skills.
- Print certificates of completion to showcase your accomplishments.

Learn more at https://education.synopsys.com.

Customer Success Community

The Black Duck Customer Success Community is our primary online resource for customer support, solutions, and information. The Customer Success Community allows users to quickly and easily open support cases and monitor progress, learn important product information, search a knowledgebase, and gain insights from other Black Duck customers. The many features included in the Customer Success Community center around the following collaborative actions:

- Connect – Open support cases and monitor their progress, as well as, monitor issues that require Engineering or Product Management assistance
- Learn – Insights and best practices from other Black Duck product users to allow you to learn valuable lessons from a diverse group of industry leading companies. In addition, the Customer Hub puts all the latest product news and updates from Black Duck at your fingertips, helping you to better utilize our products and services to maximize the value of open source within your organization.
- Solve – Quickly and easily get the answers you're seeking with the access to rich content and product knowledge from Black Duck experts and our Knowledgebase.
- Share – Collaborate and connect with Black Duck staff and other customers to crowdsource solutions and share your thoughts on product direction.

Access the Customer Success Community. If you do not have an account or have trouble accessing the system, please send an email to communityfeedback@blackducksoftware.com or call us at +1 781.891.5100 ext. 5.

To see all the ways you can interact with Black Duck Support, visit:

https://www.blackducksoftware.com/support/contact-support.

Announcements in Version 5.0.0

dependencyScan Option

As noted in the command line output and in the documentation, the **--dependencyScan** option in the Signature Scanner has been deprecated. Black Duck Software recommends using Black Duck Detect to discover declared dependencies.

In the next major release of Black Duck, the **--dependencyScan** option will be removed.

For more information, please contact your Customer Success Manager.

New Features in Version 5.0.0

Black Duck Binary Analysis

Black Duck - Binary Analysis (BDBA), a new licensed feature in Black Duck, identifies the open source security, compliance, and quality risks in the software libraries, executables, and vendor-supplied binaries in use within your codebase. BDBA supports expanded file type support including various firmware formats, filesystems/disk images, installation formats, and various compression and archive formats.

After using Black Duck Detect to scan your software or firmware, the results of your scan appear in the project version BOM. For you to easily identify these files, the BOM displays the match type as Binary.

Black Duck - Binary Analysis is supported for Docker Compose, Docker Swarm, and Kubernetes.

Audit Information

Black Duck now provides the following audit information:

- Projects now provide information on the user who:
  - Created this project and the date it was created
  - Last updated this project (by modifying any project information or by adding a member) and the date it was last updated

  This information is now available on the projects **Overview** tab.

- Project versions now provide the following information:
  - The user who created this project version and the date it was created.
  - The user who last updated this project version settings and the date it was last updated.
  - Date and time the latest scan(s) mapped to this project version completed.
  - Date and time of the last KnowledgeBase update.

  This information is now available on project version **Details** tab.

- Purpose. Users can now provide a purpose when adding or modifying a component in the BOM.
- Modification. Users can select a checkbox, and optionally add information as to why a component has been modified when adding or modifying a component to a BOM.

You can create policy rules using purpose and modification status as component conditions.

Ability to customize KnowledgeBase components

So that your BOM accurately reflects your project, users with the Component Manager role can:

- Modify Black Duck KnowledgeBase components and/or Black Duck KnowledgeBase component versions.
- Add notes to a KnowledgeBase component or component version.
- Undo these modifications and reset the KnowledgeBase data back to its original values.
- Define a status for a Black Duck KnowledgeBase component and/or component version to ensure that only approved components/versions are included in your BOM.

Policy management has been enhanced so that you can create policy rules on the status of the component or component version status.

Direct and Transitive Dependencies

Black Duck now distinguishes between direct and transitive dependencies. As such, two new match types, Direct Dependency and Transitive Dependency will now appear in project version BOMs.

The File Dependency match type will remain for any files scanned prior to release 5.0.0.

Log Files Now Automatically Purged

Log files older than 30 days are now automatically purged.

Black Duck provides a variable, DAYS_TO_KEEP_LOGS, so that you can customize this value.

New Job

A new job, CodeLocationDeletionJob, has been added. This job deletes scan and code location matches for a code location.

New Features in Version 4.8.0

New Product Name

To better reflect Black Duck Software's alignment with the Synopsys security portfolio, Hub has been renamed to Black Duck.

Cloning Project Versions

Black Duck now lets you select an existing project version and clone its component and/or security settings to the new project version. Use cloning to help reduce your workload by using the analysis and resolutions you defined in an existing project version as a baseline for a new version.

File Level License Data

A new REST API, component-license-rest-server, has been added so that you can retrieve file level license data.

User Guide

Black Duck documentation now includes a User Guide, which contains information on using Black Duck's UI.

New Job

A new job, VersionBomComputationJob, has been added which manages version BOM computation.

New Features in Version 4.7.0

Custom Components

So that your BOM accurately reflects your project, Black Duck now provides the ability to create custom components. This lets you use components in your BOM that are not available from the Black Duck KnowledgeBase, for example, if your project uses an open source component that is not tracked by the Black Duck KB.

> **Note:** Contact Black Duck Customer Support for missing versions of open source components that are managed by the Black Duck KnowledgeBase.

To identify the source of the component, a new column, **Source/Type** has been added to the `component.csv` file of the Project Version report. This column can have the value of KB_COMPONENT (for Black Duck KnowledgeBase components) OR CUSTOM_COMPONENT (for custom components).

New Component Manager Role

To accommodate the new custom component feature added in 4.7.0, a new role, Component Manager, has been added to Black Duck. Users with this role can create, edit and/or delete custom components.

Hierarchical BOM View

Black Duck now provides a hierarchical view which is based on file system relationships. Use this view to see parent components and the children subcomponents which were brought in by the parent component.

With the hierarchical view of the BOM, a new job, HierarchicalVersionBomJob, has been created to update the hierarchical version of the BOM.

New Project Field

A new optional field has been added for projects. This field, **Application ID**, can be used to store an external mapping id for the project to an external system, like an asset management system or application catalog.

New Features in Version 4.6.0

Project Creator Role

A new role, Project Creator, has been added to Black Duck. The Project Creator can create projects and project versions and can edit these projects and version settings.

New Features in Version 4.5.0

License Management

New license management options include:

- New data elements field for both custom and KnowledgeBase licenses, including License Status, Notes, and Expiration Date.
- New policy management rules capabilities for license status and expiration dates.

Snippet Matching

Customers who have purchased either the Compliance Module or the Professional Edition can now perform snippet matching. Snippet matching finds fragments of open source code used in your proprietary files or files moved into proprietary directories, and matches that code with open source code found in the Black Duck KnowledgeBase. Snippet matching does add additional scan overhead, so depending upon your usage model, additional system resources may be required for companies running multiple concurrent scans. Note that enabling snippet matching requires a registration key change. If you wish to turn this on, please contact your Black Duck representative to enable this feature.

Remediation Guidance API

The remediation guidance for a component with vulnerabilities is now available as a public API.

New Features in Version 4.4.2

Black Duck version 4.4.2 is a maintenance release, and contains no new or changed features.

New Features in Version 4.4.1

User Accounts Locked Out after 10 Failed Password Attempts

A user will be locked out of their account for 10 minutes if they fail to enter the correct password after 10 attempts. After the 10th failed attempt, a message will appear on the login page notifying the user that their account is locked.

Retaining VulnDB information

As part of the conversion from VulnDB to Black Duck Security Advisories (BDSAs), customers have the ability to retain Vulndb information associated with components found in their Bill of Materials to the external reporting database and use it for historical purposes.

Follow these instructions to capture this information:

1. Log into your Black Duck 4.4.1 system as a system admin.

2. Select **Tools** > **REST API Developers Guide**.

3. Select **vuln-db-report-db-copy-rest-server** API and then select the **/api/vulnerabilities/vulndb-copy** API.

4. Click **Try it Out!**.

   You should receive a "202 - accepted" return code.

   This will start a job that publishes your VulnDB information to your reporting database.

5. To see the progress of this job, go to the Jobs page by selecting **Administration** > **Jobs** and search for

the following job: VulndbResultsPreservationJob.

The time to complete this process will vary based on the number of projects and components found in your Black Duck instance. To verify that the data has been copied, log into your reporting database and query the following tables:

- vulndb_record
- vulndb_record_classification
- vulndb_record_reference_url

6. Once you have verified the data, contact your Black Duck Customer Support representative and ask them to update your registration key to enable the BDSA feed.

New Features in Version 4.4.0

Black Duck Security Advisories (BDSA)

Black Duck Security Advisories (BDSAs) are a Black Duck-exclusive vulnerability data feed sourced and curated by our Security Research team, part of the Black Duck Centre of Open Source Research & Innovation (COSRI) . BDSAs offer deeper coverage for a wider set of vulnerabilities than is available through the National Vulnerability Database (NVD), and provide detailed vulnerability insight, including severity, impact, exploitability metrics, and actionable remediation guidance. BDSAs are available to new Black Duck Professional customers as well as new Black Duck Security Module customers.

For more information, please contact your Customer Success Manager.

Ability to View Components with Cryptography

Black Duck now provides information to help you identify the component versions that have encryption algorithms:

- A Cryptography filter, available in the Component Dashboard and in the component version BOM page identifies those component versions with encryption.
- A new Cryptography tab, in the *Component Version* page, provides information such as a description, home page URL, originator, licensing and patent information for any component version that has encryption algorithms.
- A new Cryptography icon ( ) appears in the BOM page for any component version with encryption algorithms

> **Note:** While components added manually to existing BOMs will display cryptography information, legacy BOMs may require a rescan for cryptography data to appear.

Assess to REST APIs through an API Key

Black Duck provides the ability for you to generate one or more "tokens" for accessing Black Duck APIs. These tokens are intended to replace the use of username/password credentials in integration configurations, such as Jenkins or for the Scan Client CLI. With access tokens, if a security breach occurs, the user's credentials (which might be their SSO or LDAP credentials) are not directly compromised.

New Scan Service

For improved scalability, a new scan service has been added.

New Features in Version 4.3.1

End User License Agreement

A Registration & End-User License Agreement now appears the first time you access Black Duck. You must accept the terms and conditions to use Black Duck.

New Features in Version 4.2.0

License Management

Black Duck now provides the ability to create custom licenses. You can use this feature if you determine that a license that you use for a component in your BOM is not available from the Black Duck KnowledgeBase,

To help you manage licenses, a new License Management page has been added to Black Duck. This page displays custom licenses you have created and the licenses from the Black Duck KnowledgeBase. From this page you can view license text for any license and view the components/subprojects where specific licenses are used.

New License Manager Role

To accommodate the new license management feature added in 4.2.0, the License Manager role has been added to Black Duck. Users with this role can review, create, edit, and delete custom licenses. The new License Management page is also only visible to users with the new License Manager role.

OpenShift Support

Black Duck version 4.2.0 features support for OpenShift Enterprise 3.5 using an external database with PostgreSQL version 9.6.x.

For additional information, contact Black Duck Support.

Ability to Compare BOMs

Black Duck now provides the ability to compare the BOMS of two different versions of a project. The comparison shows the adjustments to components – new, removed, and adjusted components (components whose usage, license, or version has changed) – that occurred in the BOM and the associated change to the security risk.

Enhanced Vulnerability Data

Black Duck now reports Common Vulnerability Scoring System (CVSS) version 3.0 scores and Common Weakness Enumeration (CWE) information for security vulnerabilities.

Ability to Configure Black Duck Session Timeout Value

A new property, HUB_WEBAPP_SESSION_TIMEOUT, has been added to the hub-proxy.env file so that you can configure a session timeout value.

New Feature in Version 4.1.1

Support for IDP Metadata XML File for SAML

Black Duck now supports the ability to supply Identity Provider metadata using an xml file.

New Features in Version 4.1.0

Kubernetes Support

Black Duck version 4.1.0 features support for Kubernetes. For additional information, contact Black Duck support.

New Features in Version 4.0.0

Summary Dashboard

A new Summary Dashboard has been added to Black Duck. This dashboard provides you with a view of the overall health of the projects you have permission to view and helps you to identify areas of concern. Use this dashboard to view business critical information so you can quickly assess areas where you need to focus your attention.

External PostgreSQL Database

Black Duck now supports using Amazon Relational Database Service (RDS) for an external PostgreSQL database.

Remediation Guidance - BETA

A new Beta feature is available in Black Duck. For components in your BOM that have vulnerabilities, Black Duck provides guidance as to what other component versions are available and whether there is a version that fixes the security vulnerability that affects the component version used in your BOM. You can use this information to guide you in determining how to remediate a security vulnerability.

Cross-site Request Forgeries

Black Duck version 4.0.0 now features improved security for attempted cross-site request forgeries (CSRF).

SAML for Single Sign-On Support

Black Duck now supports the Security Assertion Markup Language (SAML) authentication protocol which enables Multi-Factor Authentication (MFA), Single Single Sign-On (SSO) and other capabilities.

Web Server Configuration Settings

You can now configure the following web server settings:

- Host port
- IPv4/IPv6

Default User Landing Page

So that you can quickly view the dashboard that interests you, the dashboard page that appears when you log

in depends on the last main dashboard (**Projects**, **Components**, **Security**, or **Summary**) you viewed prior to previously logging out.

New Features in Version 3.7.0

New Black Duck Docker Architecture

The new architecture for Black Duck is now available. This new architecture consists of "dockerizing" Black Duck so that different components are containerized which allows other orchestration tools to manage all of the individual containers. Supported orchestration tools for this release are:

- Docker Compose
- Docker Run
- Docker Swarm

You can install this version of Black Duck as a new installation or upgrade from a previous version, comprised of the old architecture.

Black Duck Docker images are available for download in the Docker Store Black Duck (https://hub.docker.com/u/blackducksoftware/) repository.

The orchestration files are located here:
https://github.com/blackducksoftware/hub/raw/master/archives/hub-docker-3.7.0.tar

The *Hub Installation Guide (Docker)* describes the installation, migration, and upgrade process.

Issue Tracker

A new Issues tab is available in the Black Duck UI. This tab displays the issues associated with a project version as monitored by an issue tracking product. Currently this feature is supported using the Black Duck-JIRA plugin (version 3.3.0 and higher).

Changed Features in 5.0.0

Custom Component Management Enhancements

The following enhancements have been made to custom component management:

- Ability to add tags to custom components/versions.
- Ability to add notes to custom components/versions.
- The date a custom component/version was last modified and the user who last modified it has been added to the Component Management table.
- Ability to select a status for a custom component/component version. By default, a custom component/version has an "Unreviewed" status.

Policy management has been enhanced so that you can create policy rules on the status of the custom component/ version status.

Operational Risk Enhancements

The following enhancements have been made to enable you to better manage operational risk:

- The number of commits for the last 12 months, the date of the last commit, and the number of contributors has been added to the KnowledgeBase *Component Version* page.
- Policy rules have been enhanced to include the commits in the past year and the contributors in the past year as component conditions when creating policy rules.

Local Logout Supported in SSO

When configuring SAML for Single Sign-On, Black Duck now supports local logout.

If this option is enabled, after logging out of Black Duck, the IDP's login page appears.

API Enhancements

- Enhanced the aggregate-bom-rest-server to obtain BOM component filters.
- Added a new REST API, component-filter-rest-server, to get the component approval status and source filters.
- Added a new REST API, component-version-filter-rest-server, to obtain the component version approval status.
- Enhanced the project-assignment-rest-server API, to obtain projects assigned to a user group.

- Added a new REST API, project-mapping-rest-server, to manage project mappings.
- Enhanced the tag-rest-server API, to support project tags.
- The endpoint for the code-location-rest-server API had a "Type" field which has been removed in release 5.0.0.
- The format of code location URIs has changed. Previously, it was a file path; now, it is a UUID. All APIs that accept or return these URIs are affected.

BOM Modifications Icon

To make it easier to discover changes, this icon () now indicates that a BOM has been modified. Hover over the icon to view more information on the modification.

Change in License Management Status

The "Conditionally Approved" license status has been changed to "Limited Approval."

Any policy rules that used this condition have been automatically updated.

Japanese Language

The 4.8.1 version of the UI, online help, and release notes has been localized to Japanese.

Changed Features in 4.8.2

Black Duck version 4.8.2 is a maintenance release and contains no new or changed features.

Changed Features in 4.8.1

Black Duck version 4.8.1 is a maintenance release and contains no new or changed features.

Changed Features in 4.8.0

New Phase for Project Versions

"Pre-release" has been added as a new phase for a project version. You can use this phase for a project that has been developed but not yet released.

Japanese Language

The 4.7.0 version of the UI, online help, and release notes has been localized to Japanese.

Changed Features in 4.7.2

Hierarchical BOM

The hierarchical BOM is now disabled by default. A new environment variable, HIERARCHICAL_VERSION_ BOM, has been added which controls whether this feature is enabled.

Changed Features in 4.7.1

Filtering the Component Dashboard

The behavior of the Component Dashboard has changed when filters are applied. When you select to filter by risk, either by using the advanced filters or by selecting a value using a risk graph:

- The risk graphs display a value of 0 for the values not selected in the filtered category.
- The values shown for the other risk categories display the corresponding values for the selected filter.

For example, if you select to filter the Component Dashboard to view only those components with high license risk, then the risk graphs for medium, low, and no license risk display a value of 0 and the risk graphs for security and operational risk display the corresponding values for those components with high license risk.

Changed Features in 4.7.0

Ability to add comments for policy overrides or removal of overrides

Black Duck now supports the ability to add comments to policy overrides or removal of overrides.

Enhancement to BOM Comparisons

The BOM Comparison feature has been enhanced so that you can now compare BOMs across projects.

Ability to Bulk Edit Snippets

Enhancements have been made to snippets that enable bulk editing of snippets in the **Source** tab.

API Enhancements

The following improvements were made to the REST APIs:

- The component-rest-server and component-version-rest-server APIs have been enhanced to manage custom components.
- Added a new REST API, project-version-bom-comparison-rest-server, to compare BOMs.

Protex BOM Tool

As part the continuing initiative to migrate users from legacy products to the latest versions of Black Duck, the link on the Tools page that imports a Protex BOM has been removed from the 4.7.0 and later versions of Black Duck. If you would like to import a Protex BOM, specify the following URL to download the Protex BOM tool zip file: https://<Black Duck hostname>/download/scan.protex.cli.zip.

Changes to Jobs

The ProtexBomJob has been replaced with the following jobs:

- GraphCompletionJob – Waits for other scan/graph jobs to finish, then kicks off the ScanCompletedJob.
- GraphInitializationJob – Merges and normalizes each scan document uploaded to Black Duck.
- ScanCompletedJob – Maps code locations to projects and kicks off the ScanAutoBomJob.
- ScanMappingJob – Maps component identifiers to Black Duck identifiers.
- ScanSignatureJob – Computes signatures for all the scanned files.

Japanese Language

The 4.6.1 version of the UI, online help, and release notes has been localized to Japanese.

Changed Features in 4.6.2

Black Duck version 4.6.2 is a maintenance release, and contains no new or changed features.

Changed Features in 4.6.1

Black Duck version 4.6.1 is a maintenance release, and contains no new or changed features.

Changed Features in 4.6.0

Supported Docker Versions

Black Duck no longer supports Docker version 17.03.x. Supported Docker versions are:

- 17.06.x
- 17.09.x
- 17.12.x
- 18.03.x

Cryptography Enhancements

The following enhancements have been made to the cryptography feature:

- The **Crypto** tab now includes algorithm ID, algorithm name, key length type, and key length information.
- A new file, `crypto.csv` has been added to the Project Version report. This file lists the cryptography information for each component in the project version, including the algorithm ID, algorithm name, key length type, and key length.

License Management Enhancement

A license status filter has been added to the License Management page. Possible status values are:

- Unreviewed
- Approved
- Rejected
- Conditionally Approved

API Enhancement

The following improvement was made to the REST APIs:

- Added a new REST API, tag-rest-server, for tag management.

Japanese Language

The 4.4.1 version of the UI, online help, and release notes has been localized to Japanese.

Changed Features in 4.5.1

Black Duck version 4.5.1 is a maintenance release, and contains no new or changed features.

Changed Features in 4.5.0

Expanded User Roles

Black Duck Version 4.5.0 adds new user roles. The User Role Matrix is expanded with new user roles to provide additional granularity and flexibility in setting up and managing users, projects, and rights.

New Authentication Service

A new authentication service for Black Duck 4.5.0 adds a new Docker container. This provides additional resources, and hands off the authentication.

Changed Features in 4.4.2

Black Duck version 4.4.2 is a maintenance release, and contains no new or changed features.

Changed Features in 4.4.1

NTLM Support for the Black Duck Scan Client

Black Duck scan client now supports NTLM authentication.

User Login Information included in Log Files

Logs now contain information by username on successful logins, unsuccessful logins, and account lockouts.

Link to National Vulnerability Database Web Page added to Vulnerability Detail Pages

The vulnerabilities detail pages now have a link to the CVE web page maintained by the NVD for vulnerabilities that have associated CVEs.

Changed Features in 4.4.0

Enhancements to License Management

Black Duck now provides the ability for License Managers to globally modify the license family and text of KnowledgeBase licenses. License Managers can also restore these modified KnowledgeBase licenses to their original values.

Change in Hardware Requirements

For better performance, the minimum CPUs for installation of Black Duck has been increased from 4 to 5 CPUs.

Dependency Detection Optional in Black Duck Scanner

Dependency detection is now optional in the Signature Scanner. In the command line version of the Signature Scanner, use the new **--dependencyScan** option to enable scanning for declared dependencies.

Instead of using the **--dependencyScan** option, Black Duck recommends using Black Duck Detect to discover declared dependencies.

SAML Enhancement

You can now select to synchronize groups, whereby, upon login, groups from IDP are created in Black Duck and users will be assigned to those groups.

Column renamed in Project Version Report

Prior to Black Duck 4.4.0, the components.csv file in the Project Version report, had two columns titled "Origin id". As of 4.4.0, the second "Origin id" column has been renamed to "Origin name id".

API Enhancements

The following improvements were made to the REST APIs:

- Added a new REST API, api-token-rest-server, for use of the APIs through an API key.
- Improved the component-version-rest-server API, to obtain cryptography information.
- Added a new REST API, scan-service-proxy-rest-server, to obtain and post scan information. This REST API replaces the scan-rest-server REST API.
- Removed the autocomplete functionality from the search-rest-server API.

Enhancement to Report Database

The report database has added a new column, `related_vuln_db`, to the Component Vulnerability Table. This column provides access to the related CVE vulnerability for a BDSA.

Docker Run

Docker Run support is deprecated.

Japanese Language

The 4.3.1 version of the UI, online help, and release notes has been localized to Japanese.

Black Duck Integrations

Go to the GitHub website (https://github.com/blackducksoftware/integration-all/) to view available Black Duck integrations.

Enhancement to Jobs page

The Jobs page now includes a **Related to** column which provides links so that you can determine what some jobs are related to.

Changed Features in 4.3.0

Code Locations changed to Scans

To better reflect functionality, the menu and text in the Black Duck UI has been changed from **Code Locations** to **Scans**.

> **Note:** For the Project Version report, the codelocations.csv file is now the scans.csv file. In this file, the first column was changed from "Code location id" to "Scan id" and the tab name has changed from "codelocations" to "scans".

Enhancements to Policy Management

The following enhancements have been made to policy management:

- Provided the ability to copy policy rules.
- Provided the ability to individually override policy rules.
- Hovering over the Policy Violation icon (⊘) now lists the individual policy rules that were violated.
- Added the ability to create a policy rule based on the component release date.
- The Policy Management page now has a filter so that you can select to view only enabled or disabled policy rules. Enabled rules are displayed by default.
- More details have been added to policy violation notifications.

Enhancements to Group Management

To let you quickly see the projects assigned to a group, the *Group Name* page now includes the **Group Projects** sections which lists the projects that this group is assigned to. Users with the sysadmin role can use this page to add or remove projects from a group.

Enhancement to User Management

- To let you quickly view the roles assigned to a user, each user's roles are now listed on the User Management page.
- So that you can easily view the projects assigned to a user, the *Username* page now includes the **Projects Access** section which shows the projects assigned to the user.

Phase Filter Added to Project Version Page

To help you view the project versions that interest you, a filter has been added to the Project Version page that lets you filter the versions shown on the page by release phase.

Enhancement to Scans page

The ability to sort by the **Scan Size** and **Mapped to** columns has been added to the Scans page.

Identical Queued Scans Now Skipped

Automation can push many scans for the same code to Black Duck causing these scans to get queued up. Now when this occurs, any non-started scans will be skipped so that the latest scan can execute faster.

API Enhancements

The following improvements were made to the REST APIs:

- Improved the notification-rest-server API to update the state of notifications.
- Added a new REST API, policy-rule-filter-rest-server, for retrieving enabled policy rules.
- Improved the user-rest-server API to obtain the current user.

- Improved the user-group-rest-server API to manage groups and users in groups: creating updating, and deleting groups and adding or removing users from groups.

Installation Guides

To make it easier to use the documentation, there are now these installation guides:

- *Installing Hub using Docker Swarm*
- *Installing Hub using Docker Compose*
- *Installing Hub using Kubernetes*

Japanese Language

The 4.2.0 version of the UI, online help, and release notes has been localized to Japanese.

Black Duck Integrations

Go to the GitHub website (https://github.com/blackducksoftware/integration-all/) to view available Black Duck integrations.

Tools Page Reorganization

The Tools page has been reorganized:

- To download the original Scanner and CLI, click **CLI** to download the Linux, Mac OS X, or Windows version of the Signature Scanner.
- To download the Scanner 2.0, click **Desktop** to download the Mac OS X or Windows version of the Signature Scanner.

Improved Usability

Various usability improvements have been made to Black Duck to increase consistency across the application and make it easier to use.

Changed Features in 4.2.0

PostgreSQL version

For Black Duck version 4.2.0, the currently-supported version of PostgreSQL is 9.6.x, which is the version supplied in Black Duck's PostgreSQL container. If you choose to run your own PostgreSQL instance, you must be at PostgreSQL version 9.6.x for compatibility with Black Duck version 4.2.0.

If you are upgrading from a previous version of Black Duck, you will need to run a migration script prior to upgrading to version 4.2.0. Refer to the *Black Duck Hub Installation Guide* for more information.

LDAP Configuration

You no longer have to manually manage the certificate exchange. You can now use Black Duck UI to manage the certificate exchange between the LDAP server and Black Duck.

Subprojects Information Included in Reports

Reports now include subproject information for users that have permission to the subproject.

Enhancement to Policy Rules

You can now create a policy rule based on the review status of a component.

Japanese Language

The 4.1.0 version of the UI, online help, and release notes has been localized to Japanese.

API Enhancements

The following improvements were made to the REST APIs:

- Improved the license-rest-server API to provide the ability to update and delete licenses and update license text.
- Improved the aggregate-bom-rest-server API, to add BOM components.
- Improved the vulnerability-rest-server API, to obtain Common Weakness Enumeration (CWE) information.
- Added a REST API, meta-rest-server, to provide the current version of Black Duck.

Black Duck Integrations

The following Black Duck integrations are now available from the GitHub website (https://github.com/blackducksoftware/integration-all/):

- Black Duck Artifactory Plugin
- Black Duck Bamboo Plugin
- Black Duck Gradle Plugin
- Black Duck Eclipse Plugin
- Black Duck Jenkins Plugin
- Black Duck JIRA Plugin
- Black Duck Maven Plugin
- Black Duck NuGet Plugin
- Black Duck PIP Plugin
- Black Duck SBT Plugin
- Black Duck Team City Plugin
- Black Duck Team City Foundation Server Plugin
- Black Duck Visual Studio Plugin
- Black Duck Email Extension
- Black Duck Docker Inspector
- Black Duck Detect

Note: For complete information on Black Duck integration products, including the latest release version number, refer to the Black Duck Integrations documentation website (https://blackducksoftware.atlassian.net/wiki/spaces/INTDOCS/overview).

Improved Usability

Various usability improvements have been made to Black Duck to increase consistency across the application and make it easier to use.

Changed Features in 4.1.2

Logging out of Black Duck

Black Duck does not support SP-Initiated IdP logout (SLO). When SSO users log out of Black Duck, a logout page now appears notifying them that they successfully logged out of Black Duck. This logout page includes a link to log back into Black Duck; users may not need to provide their credentials to successfully log back in to Black Duck.

Changed Features in 4.1.0

New Signature Scanner 2.0 - BETA

A Beta version of the Signature Scanner - 2.0 is now available from the Tools page of the Black Duck UI.

API Enhancements

The following improvement was made to the REST APIs:

- Added review status to public BOM API.
- Added policy status to public component BOM API.
- Improved the user-group-rest-server API to add, edit, and remove a role.
- Added a REST API, project-assignment-rest-server, to assign and remove users and user groups from projects.
- Improved the component-version-rest-server and aggregate-bom-rest-server APIs to provide actual license text for components.

Documentation container

The documentation for Black Duck is now managed in a container which will enable faster updates to the documentation.

LDAP logging

Black Duck log files now indicate if LDAP is enabled or disabled.

PostgreSQL version

For Black Duck version 4.1.0, the currently-supported version of PostgreSQL is 9.4.11, which is the version supplied in Black Duck's PostgreSQL container. If you choose to run your own PostgreSQL instance, you must be at PostgreSQL version 9.4.11 for compatibility with Black Duck version 4.1.0.

For Black Duck versions higher than 4.1.0, be sure to check the *Black Duck Release Notes* for possible updated PostgreSQL version requirements prior to upgrading.

Black Duck Integrations

New versions of the following Black Duck integrations are now available from the GitHub website

(https://github.com/blackducksoftware/integration-all/):

- Black Duck Artifactory Plugin
- Black Duck Bamboo Plugin
- Black Duck Gradle Plugin
- Black Duck Jenkins Plugin
- Black Duck JIRA Plugin
- Black Duck Maven Plugin
- Black Duck NuGet Plugin
- Black Duck PIP Plugin
- Black Duck Team City Plugin
- Black Duck Team City Foundation Server Plugin
- Black Duck Eclipse Plugin
- Black Duck Visual Studio Plugin
- Black Duck Email Extension
- Black Duck Docker Inspector
- Black Duck SBT Plugin

Note: For complete information on Black Duck integration products, including the latest release version number, refer to the Black Duck Integrations documentation website (https://blackducksoftware.atlassian.net/wiki/spaces/INTDOCS/overview).

Changed Features in 4.0.0

Improvements to the Notices File Report

To simplify the creation of the Notices File report, Black Duck now displays and reports on the actual license text for licenses which are typically modified for each OSS component. Currently, Black Duck provides the actual license text for the MIT, variants of the BSD, and the ISC licenses, which are the top components in our KnowledgeBase, based upon customer usage.

New Black Duck Module

A new module, the OSS Notices Report, is now available and the existing OSS Attribution module has been modified. The Notices File report is now included with this new OSS Notices Reports module which is part of the License Compliance offering. If you do not have the OSS Notices Reports module, the Notices File report is no longer available to you.

Improvements to the Report Database

The report database now provides access to the policy approval status, usage, and match type for a component.

Signature Scanner Command Line Improvements

- The **dryRunReadFile** parameter can now be used to upload individual BOM (.jsonld) files, without the corresponding scan container (.json) file.

- The **password** parameter is no longer supported. If you supply an argument to the **password** parameter, the scan will not complete. Instead, you must set the BD_HUB_PASSWORD environment variable with Black Duck server password.

Improvements to Scanning Containers

The script used to scan Docker images, `scan.docker.sh`, has been improved to include package manager level inspection. Also, an automatic update feature has also been added to the script so that you can easily obtain the latest version of this script.

> **Note:** To take advantage of the automatic update feature now available in this script, you need to ensure connectivity (via whitelisting or other means) to the github.com domain (blackducksoftware.github.com).

Commercial Components

Commercial components are now identified as such in search results.

Basic Authentication Support

Black Duck now supports basic authentication for a proxy.

Scanning Improvements

Enhanced matching algorithms and new Black Duck KB data elements have been added to improve matching accuracy with fewer false positives. This applies to many types of scans, but is particularly effective with Debian packages.

Japanese Language

The 3.7.0 version of the UI, online help, and release notes has been localized to Japanese.

Black Duck Integrations

New versions of the following Black Duck integrations are now available from the GitHub website (https://github.com/blackducksoftware/integration-all/):

- Artifactory Plugin version 3.0.0 and later
- Bamboo Plugin version 3.1.0 and later
- Gradle Plugin version 5.0.1 and later
- Jenkins Plugin version 2.2.1 and later
- JIRA Plugin version 3.3.1 and later
- Maven Plugin version 2.0.1 and later
- NuGet Plugin version 1.1.0 and later
- Pip Plugin version 1.1.0 and later
- Team City Plugin version 3.1.0 and later

Improved Usability

Various usability improvements have been made to Black Duck to increase consistency across the application and make it easier to use.

Changed Features in 3.7.0

Improvement to the Report Database

The report database now provides access to component vulnerability data. It also includes data as to whether a component version is ignored.

Enhancements to Policy Rules

The "does not equal" and "not in" operators have been added for component version policy rules. With these operators, you can now more easily create whitelist policy rules, such as creating a policy rule that triggers a policy violation when a specific versions of a component are *not* used.

Code Scanner Role

The code scanner role has been modified. Users with only this role can no longer see the BOMs associated with the code location scans.

API Enhancements

The following improvement was made to the REST APIs:

- Added a REST API, bom-component-issue-rest-server, to add, update, and delete issues for component versions.

Black Duck Integrations

New versions of the following Black Duck integrations are now available from the GitHub website (https://github.com/blackducksoftware/integration-all/):

- Eclipse Plugin version 1.0.0 and later
- Gradle Plugin version 5.0.0 and later
- JIRA Plugin version 3.3.0 and later
- NuGet Plugin version 1.0.0 and later
- Pip Plugin version 1.0.0 and later
- SBT Plugin version 1.1.0 and later
- Team City Plugin version 3.0.2 and later
- Visual Studio Plugin version 1.0.0 and later

Japanese Language

The 3.6.0 version of the UI, online help, and release notes has been localized to Japanese.

Improved Usability

Various usability improvements have been made to Black Duck to increase consistency across the application and make it easier to use.

Fixed Issues in 5.0.0

The following customer-reported issues were fixed in this release:

- Fixed an issue when using SAML, Google's G_Suite did not redirect to Google for authentication.
- Fixed an issue whereby project and project version settings were not visible using IE 11.
- Fixed an issue whereby notifications could not be retrieved using the API when the code scan limit warning appeared.
- Fixed an issue whereby the system_check.sh script was failing.
- Logs downloaded from the Black Duck UI now includes zookeeper logs.
- Fixed an issue with the Kubernetes installation so that the webserver init script now skips the chowns of user-provided secrets for nginx.
- Fixed an issue whereby only 10 project were shown in the Add Projects dialog box.
- Performance has been improved when loading the hierarchical BOM.
- Fixed an issue whereby an error was not shown when you attempted to add the same project more than once to a group.
- Fixed an issue whereby the Group Membership column in the User Management page displayed the same group name multiple times.
- Fixed an issue with roles whereby a user could view projects that they did not have access to.
- Fixed an issue whereby snippet matching never finished successfully.
- Fixed an issue so that more than 100 users now appear in the owner list on the *Project Name* **Settings** tab.
- Fixed an issue generating a vulnerability report for a project when a subproject had a component match type not present in the main project.

Fixed Issues in 4.8.2

The following customer-reported issues were fixed in this release:

- Fixed an issue whereby accessing a direct link to a scan brought you to the Black Duck login page instead of the SSO login page.
- Fixed an issue whereby a GraphInitializationJob error appeared when scanning files.
- Fixed an issue whereby the jobrunner container was constantly restarting.
- Fixed an issue whereby the Black Duck Scanner displayed an "Internal Server Error" when scanning or

uploading a file.

- Fixed an issue whereby long external IDs were truncated.
- Fixed an issue with the project-rest-server API whereby the offset value was calculated incorrectly.
- Fixed an issue whereby deadlock errors occurred on scan jobs.

Fixed Issues in 4.8.0

The following customer-reported issues were fixed in this release:

- The vulnerability API is now returning CVSS2 scores when the score is available in Black Duck.
- Fixed an issue whereby users with the global code scanner role could not delete a report that they had created.
- Fixed an issue whereby a user configuring LDAP using the Black Duck UI would receive a 502 error code message.
- Fixed an issue whereby the rows in a report incorrectly indicated that the rows were already expanded.
- Fixed an issue whereby the database backup did not honor symbolic links.
- Fixed an issue whereby a user with the superuser role could not view a project.
- Fixed an issue with the page layout of the BOM Comparison page.

Fixed Issues in 4.7.1

The following customer-reported issues were fixed in this release:

- Fixed the labels in the Black Duck Scanner so that would display correctly when the browser's language setting is Japanese.
- Improved the performance of the project version **Security** tab.
- Fixed an issue whereby a row in the BOM table would shift when a comment was saved and before the comment icon was displayed.
- Fixed an issue whereby the tooltips on the BOM page would not close.
- Fixed an issue where a large header caused a 400 Bad Request error from NGINX.
- Fixed an issue whereby a user with the Global Code Scanner or Project Creator role received a "No results found" message on the **Affected Projects** tab.
- Improved the performance of the Component Dashboard when displaying a large number of components.
- Improved the performance of the Project Versions page when displaying a large number of versions.

Fixed Issues in 4.7.1

The following customer-reported issues were fixed in this release:

- Improved the performance of the project version **Security** tab.
- Fixed an issue whereby the tooltips on the BOM page would not close.
- Improved the performance of the **Components** tab when displaying a large number of components.

Fixed Issues in 4.7.0

The following customer-reported issues were fixed in this release:

- Fixed an issue whereby the scan status was not being updating to FAILED for orphan jobs that were rescheduled.
- Fixed an issue whereby a vulnerability report for a specific date range contained vulnerabilities that had not been updated nor changed.
- Fixed an issue where the **Scan Initiated By** field in the *Scan Name* page was not populated.
- Fixed an issue whereby the job status shown on the Jobs page was incorrect in some cases.
- Fixed an issue in the group member table whereby special characters, such as an apostrophe, in user names displayed the URL encoding for the character.
- Fixed issues with the **Affected Projects** tab so that it now sorts components and projects correctly.
- Fixed an issue whereby scans would not upload in the Black Duck UI when using Internet Explorer 11.
- Fixed an issue whereby the createVersionReport API did not work correctly unless cryptography was enabled.
- Fixed an issue whereby the BOM displayed a "No Results Found" message if you used a 2-step process to scan and then map the scan to a project.
- Fixed an issue whereby the BOM was not populated when a larger scan file was uploaded and linked to a project version after the scan's state was 'Complete'.
- Fixed an issue whereby the Sysadmin user could not be added as a project member.
- Fixed an issue with the UI that prevented a policy rule from being copied.
- Fixed an issue with a failing KbReleaseUpdateJob and the Black Duck KnowledgeBase failing to respond.
- Fixed an issue with the findBomComponentVersion API which returned a 400 error code when the component version in the BOM had a 'Reviewed' status.

Fixed Issues in 4.6.2

The following customer-reported issues were fixed in this release:

- Fixed an issue whereby the overall roles in an existing group could not be changed.
- Fixed an issue so that the performance of the Project dashboard improved.

Fixed Issues in 4.6.0

The following customer-reported issues were fixed in this release:

- Fixed an issue with the Vulnerability Status Report, Vulnerability Update Report, Vulnerability Remediation Report, and the project version reports so that they now exclude ignored components by default.
- Fixed an issue so that email addresses are no longer required when creating or editing users.
- Fixed an issue whereby the scan status for orphaned scan jobs was not updated.
- Fixed an issue whereby vulnerability reports included vulnerabilities that were not updated or changed.
- Fixed an issue whereby the BOM Comparison page occasionally incorrectly indicated that licenses were modified.

- Fixed an issue whereby scan jobs lasting longer than 24 hours displayed an incorrect duration on the Jobs page in the Black Duck UI.

Fixed Issues in 4.5.0

The following customer-reported issues were fixed in this release:

- Fixed an issue wherein a Black Duck production environment using Docker Swarm may not be able to connect to an external database.
- Fixed an issue wherein the Scan page may be blank when a scan is in progress.
- Fixed an issue wherein multiple users in the same group and having the same permissions may see different search results.
- Fixed an issue wherein some APIs were not returning the code location size.
- Fixed an issue wherein logs in logstash may not be created in a Black Duck cluster.
- Fixed an issue wherein the Add Comment text box did not have a focused cursor.
- Fixed an issue wherein running Black Duck Scanner 2.0 may display an *Unable to verify first certificate* error.
- Fixed an issue in the Protex BOM tool user interface description which now displays the correct required Java version, which is JRE 1.8.x or higher.
- Fixed an issue wherein the JobRunner may disconnect in Black Duck version 4.3.1.
- Fixed an issue wherein hosted Black Duck customers be unable to scan using the CLI.
- Fixed an issue wherein the Component Review flag was not persisting on all components.
- Fixed an issue wherein the References page may display as blank when attempting to view the details of a vulnerability database entry.

Fixed Issues in 4.4.3

The following customer-reported issues were fixed in this release:

- Resolved an issue wherein under certain circumstances, Black Duck may display a blank page.

Fixed Issues in 4.4.2

Black Duck version 4.4.2 was a maintenance release, and contained no customer-reported fixed issues.

Fixed Issues in 4.4.0

The following customer-reported issues were fixed in this release:

- Docker Containers now have their root file system mounted as read only.
- Fixed an issue whereby notifications were received on ignored components.
- Fixed a discrepancy between what was displayed on the BOM page versus the Source page for component versions with multiple licenses.
- REST API sorting now works on releasedOn and versionName parameters.
- Fixed an issue whereby large scans caused deadlock errors in Job Runner.

Fixed Issues in 4.3.1

The following customer-reported issue was fixed in this release:

- Fixed an issue whereby the job runner container became disconnected when running Black Duck with a multi-node Docker Swarm cluster.

Fixed Issues in 4.3.0

The following customer-reported issue was fixed in this release:

- Fixed an issue where Solr would not start as the solr container did not clean stray lock files before startup.

Fixed Issues in 4.2.0

The following customer-reported issues were fixed in this release:

- The Security tab now displays the list of vulnerabilities by descending order of the base score so that the more severe vulnerabilities are now at the top of the page and easier to locate.
- Fixed a timeout issue where the Black Duck UI displayed "The Hub server did not respond in time" message when loading component matches in the Code Location page.
- A scan status has been added to the header on the BOM page to indicate whether the scan has succeeded or failed.
- The NVD URL link provided in the `security.csv` report has been updated.
- Fixed an issue where users could not edit the reviewed components checkbox in a project version BOM.
- Fixed an issue whereby a project member with no other roles could not create a comment.
- The Web API documentation for the report API now provides information on what options are available for each request parameter.
- Fixed an issue with the reporting database whereby a reporting database transfer job was failing.
- Fixed an issue with the vulnerability API capping the number of results to 100 items.
- Fixed an issue with email addresses in Active Directory causing the incorrect user avatar to be displayed.
- Fixed an issue with the code-location-rest-server API whereby the sorting order was not working correctly.
- Fixed an issue where the KBVulnerabilityVdbUpdateJob shown on the Jobs page displayed an error status every 30 minutes.
- Fixed an issue whereby vulnerability reports were failing for a project with a large number of components.

Fixed Issues in 4.1.1

The following customer-reported issues were fixed in this release:

- Fixed an issue where the total scan size did not equal the reported scan size as shown on the Code Locations page.
- Fixed an issue where license risk was not recalculated after the project distribution was changed.
- Fixed an issue when creating a policy rule where selecting additional licenses or projects removed the

previous selection.

- Fixed an issue with the reporting database whereby a reporting database transfer job was failing.

Fixed Issues in 4.1.0

The following customer-reported issues were fixed in this release:

- Fixed an issue with Docker containers not starting due to possible version incompatibilities with older version of CentOS.
- Fixed an issue which may have caused failures when using the BOM import/export tool to import a Bill of Materials (BOM).
- Fixed an issue in the REST API wherein the **** character was not properly encoded in JSON output.
- Fixed an issue wherein match type changes made in Black Duck user interface were not always propagating to reports.
- Fixed an issue wherein BOM paths containing Chinese characters may fail.

Fixed Issues in 4.0.0

The following customer-reported issues were fixed in this release:

- Fixed an issue with the formatting of the text version of the Notices Report file.
- Fixed an issue with Black Duck reports which displayed an incorrect column title for the component name.
- Fixed an issue whereby the Signature Scanner would fail if its own path contained a space.
- Exclude patterns now work when scanning on Windows.
- The Signature Scanner no longer inserts a <%=moduleName%> tag in a .jsonld file.
- Fixed an issue whereby the script used to create custom certificates did not create a permanent image of the container used to save the certificate configuration changes.

Fixed Issues in 3.7.1

The following customer-reported issues were fixed in this release:

- Fixed an issue with the reporting database whereby a reporting database transfer job was failing.
- Fixed a usability issue so that on a Mac, you can use the CMD key when selecting a link to open the link in a new tab.
- The Registration page now displays the correct code base limit.

The following is a list of known issues and limitations in Black Duck:

- The media types shown in the REST API Developers Guide documentation may be incomplete.
- If you notice performance issues, do the following:
  1. Log into the server that is running the docker container.
  2. Determine the container ID:

     ```
     docker ps | grep postgres
     ```

  3. Start PostgreSQL against the docker container.

     ```
     docker exec -it <container id> psql -d bds_hub
     ```

  4. At the Postgres prompt, execute the following query:

     ```
     ALTER SYSTEM SET max_wal_size - '8GB'
     ```

  5. Restart Black Duck.

- Searching for a project by name in Black Duck may not display any results. To resolve this issue:
  1. Log in to Black Duck with the System Administrator role and select **Administration** from the expanding menu icon ( ).
  2. Select **System Settings**.
  3. Click **Reindex** which will reindex the projects and resolve this issue.

- If you are using an LDAP directory server to authenticate users, consider the following:
  - Black Duck supports a single LDAP server. Multiple servers are not supported.
  - If a user is removed from the directory server, Black Duck user account continues to appear as active. However, the credentials are no longer valid and cannot be used to log in.
  - If a group is removed from the directory server, Black Duck group is not removed. Delete the group manually.

- Tagging only supports letters, numbers, and the plus (+) and underscore (_) characters.
- If Black Duck is authenticating users, user names are not case sensitive during login. If LDAP user authentication is enabled, user names are case sensitive.
- If a code location has a large bill of materials, deleting a code location may fail with a user interface timeout error.