




# **BLACKDUCK** | Hub

## Release Notes

Version 4.5.1



This edition of the *Release Notes* refers to version 4.5.1 of the Black Duck Hub.

This document created or updated on Monday, April 2, 2018.

**Please send your comments and suggestions to:**

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

Copyright © 2018 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 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.

<b>Chapter 1: New Features</b>	<b>1</b>
New Features in Version 4.5.0	1
License Management	1
Snippet Matching	1
Remediation Guidance API	1
New Features in Version 4.4.2	1
New Features in Version 4.4.1	1
User Accounts Locked Out after 10 Failed Password Attempts	1
Retaining VulnDB information	1
New Features in Version 4.4.0	2
Black Duck Security Advisories (BDSA)	2
Ability to View Components with Cryptography	2
Assess to REST APIs through an API Key	3
New Scan Service	3
New Features in Version 4.3.1	3
End User License Agreement	3
New Features in Version 4.2.0	3
License Management	3
New License Manager Role	3
OpenShift Support	3
Ability to Compare BOMs	4
Enhanced Vulnerability Data	4
Ability to Configure Hub Session Timeout Value	4
New Feature in Version 4.1.1	4
Support for IDP Metadata XML File for SAML	4
New Features in Version 4.1.0	4
Kubernetes Support	4
New Features in Version 4.0.0	4
Summary Dashboard	4
External PostgreSQL Database	4
Remediation Guidance - BETA	4
Cross-site Request Forgeries	4
SAML for Single Sign-On Support	5

Web Server Configuration Settings .....	5
Default User Landing Page .....	5
New Features in Version 3.7.0 .....	5
New Hub Docker Architecture .....	5
Issue Tracker .....	5
New Features in Version 3.6.0 .....	5
Beta for the New Hub Docker Architecture .....	5
Report Database .....	6
Output the BOM Display to a PDF File .....	6
Ability to add projects to a BOM .....	6
Dockerized Scan Client .....	6
New Features in Version 3.5 .....	7
Adding Comments to a BOM .....	7
Review Flags in a BOM .....	7
Code Location Names .....	7
Viewing Discovery Source .....	7
Support for Oracle Enterprise Linux 7 .....	7
New Features in Version 3.4.2 .....	8
Hub Email Extension .....	8
New Hub Integration .....	8
New Features in Version 3.4 .....	8
New OSS Attribution Module .....	8
Package Manager Support .....	8
Better Matching for Linux Distributions .....	8
New Features in Version 3.3.2 .....	8
Ability to Access the REST APIs from a Web Page Served from a non-Hub Server .....	8
New Features in Version 3.3.1 .....	9
Extension Support .....	9
Code Size Limit Notification .....	9
API Enhancement .....	9
New Features in Version 3.3.0 .....	9
Notices File Report .....	9
Feedback Service .....	9
Support for Maven and Gradle Projects .....	9
API Enhancements .....	9
Operating System Support .....	9
Hub Integrations .....	10
New Features in Version 3.2.0 .....	10
Subcomponent Discovery .....	10
Ability to View Files Affected by a Vulnerability .....	10
Hub Integrations .....	10

<b>Chapter 2: Changed Features</b>	<b>11</b>
Changed Features in 4.5.1	11
Changed Features in 4.5.0	11
Expanded User Roles	11
New Authentication Service	11
Changed Features in 4.4.2	11
Changed Features in 4.4.1	11
NTLM Support for the Hub Scan Client	11
User Login Information included in Log Files	11
Link to National Vulnerability Database Web Page added to Vulnerability Detail Pages	11
Changed Features in 4.4.0	12
Enhancements to License Management	12
Change in Hardware Requirements	12
Dependency Detection Optional in Hub Scanner	12
SAML Enhancement	12
Column renamed in Project Version Report	12
API Enhancements	12
Enhancement to Report Database	12
Docker Run	12
Japanese Language	12
Hub Integrations	13
Enhancement to Jobs page	13
Changed Features in 4.3.0	13
Code Locations changed to Scans	13
Enhancements to Policy Management	13
Enhancements to Group Management	13
Enhancement to User Management	13
Phase Filter Added to Project Version Page	13
Enhancement to Scans page	14
Identical Queued Scans Now Skipped	14
API Enhancements	14
Installation Guides	14
Japanese Language	14
Hub Integrations	14
Tools Page Reorganization	14
Improved Usability	14
Changed Features in 4.2.0	15
PostgreSQL version	15
LDAP Configuration	15
Subprojects Information Included in Reports	15
Enhancement to Policy Rules	15

Japanese Language .....	15
API Enhancements .....	15
Hub Integrations .....	15
Improved Usability .....	16
Changed Features in 4.1.2 .....	16
Logging out of the Hub .....	16
Changed Features in 4.1.0 .....	16
New Hub Scanner 2.0 - BETA .....	16
API Enhancements .....	16
Documentation container .....	17
LDAP logging .....	17
PostgreSQL version .....	17
Hub Integrations .....	17
Changed Features in 4.0.0 .....	17
Improvements to the Notices File Report .....	17
New Hub Module .....	18
Improvements to the Report Database .....	18
Hub Scanner Command Line Improvements .....	18
Improvements to Scanning Containers .....	18
Commercial Components .....	18
Basic Authentication Support .....	18
Scanning Improvements .....	18
Japanese Language .....	18
Hub Integrations .....	19
Improved Usability .....	19
Changed Features in 3.7.0 .....	19
Improvement to the Report Database .....	19
Enhancements to Policy Rules .....	19
Code Scanner Role .....	19
API Enhancements .....	19
Hub Integrations .....	19
Japanese Language .....	20
Improved Usability .....	20
Changed Features in 3.6.1 .....	20
Hub Integrations .....	20
Changed Features in 3.6.0 .....	20
Severity Level Added to Policies .....	20
Improvements to the Hub Scanner .....	20
The Protex BOM Tool .....	21
Read-only user role .....	21
API Enhancements .....	21

Hub Integrations .....	21
Hub Email Extension .....	21
Japanese Language .....	21
Improved Usability .....	22
Changed Features in 3.5 .....	22
Improvements to the Hub Scanner .....	22
API Enhancements .....	22
Hub Integrations .....	22
Hub Email Extension .....	22
Japanese Language .....	22
Improved Usability .....	22
Changed Features in 3.4.2 .....	23
API Enhancements .....	23
Hub Integrations .....	23
Changed Features in 3.4 .....	23
Modifications to Notices File Report .....	23
Improvements to the Hub Scanner .....	23
Additional Remediation Status .....	23
Ability to View a User's Groups .....	23
Scan Size Limits .....	24
API Enhancements .....	24
Retention of Historical Scans .....	24
Hub Integrations .....	24
Improved Usability .....	24
Japanese Language .....	24
Current KnowledgeBase Statistics .....	24
Changed Features in 3.3.1 .....	25
Improvements to the Hub Scanner .....	25
Notification Enhancements .....	25
Additional Operand for Policy Rules .....	25
Hub Integrations .....	25
Changed Features in 3.3.0 .....	25
Additional Conditions for Policy Rules .....	25
Improvements to the Hub Scanner .....	26
Additional Usage Types .....	26
Improvements to Component Scanning and Identification .....	26
Configurable Admin Console .....	26
Japanese Language .....	26
Improved Usability .....	26
Changed Features in 3.2.0 .....	26
Improvements to the Hub Scanner .....	26

Improved Usability .....	27
<b>Chapter 3: Fixed Issues .....</b>	<b>28</b>
Fixed Issues in 4.5.0 .....	28
Fixed Issues in 4.4.3 .....	28
Fixed Issues in 4.4.2 .....	28
Fixed Issues in 4.4.0 .....	28
Fixed Issues in 4.3.1 .....	29
Fixed Issues in 4.3.0 .....	29
Fixed Issues in 4.2.0 .....	29
Fixed Issues in 4.1.1 .....	30
Fixed Issues in 4.1.0 .....	30
Fixed Issues in 4.0.0 .....	30
Fixed Issues in 3.7.1 .....	30
Fixed Issues in 3.6.1 .....	31
Fixed Issues in 3.6.0 .....	31
Fixed Issues in 3.5.2 .....	31
Fixed Issues in 3.5 .....	31
Fixed Issues in 3.4.2 .....	31
Fixed Issues in 3.4 .....	31
Fixed Issues in 3.3.0 .....	32
Fixed Issues in 3.2.0 .....	32
<b>Chapter 4: Known Issues and Limitations .....</b>	<b>33</b>



## The Hub documentation

The documentation for the Hub consists of online help and these documents:

Title	File	Description
Release Notes	release_notes_bd_hub.pdf	Contains information about the new and improved features, resolved issues, and known issues in the current and previous releases.
Installing Hub using Docker Compose	hub_install_compose.pdf	Contains information about installing and upgrading the Hub using Docker Compose.
Installing Hub using Docker Swarm	hub_install_swarm.pdf	Contains information about installing and upgrading the Hub using Docker Swarm.
Installing Hub using Kubernetes	hub_install_kubernetes.pdf	Contains information about installing and upgrading the Hub using Kubernetes.
Installing Hub using OpenShift	hub_install_openshift.pdf	Contains information about installing and upgrading the Hub using OpenShift.
Getting Started	hub_getting_started.pdf	Provides first-time users with information on using the Hub.
Scanning Best Practices	hub_scanning_best_practices.pdf	Provides best practices for scanning.
Getting Started with the Hub SDK	getting_started_hub_sdk.pdf	Contains overview information and a sample use case.
Report Database	report_db_bd_hub.pdf	Contains information on using the report database.

Hub integration documentation can be found on [Confluence](#).

## Training

Black Duck Academy 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 Black Duck Academy, 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://www.blackducksoftware.com/services/training>

View the full catalog of courses and try some free courses at <https://academy.blackducksoftware.com>

When you are ready to learn, log in or sign up for an account: <https://academy.blackducksoftware.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](mailto: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>.

## 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

Hub 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 Hub 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 Hub 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 Hub Professional customers as well as new Hub Security Module customers.


For more information, please contact your Customer Success Manager.

### Ability to View Components with Cryptography

The Hub 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

The Hub provides the ability for you to generate one or more “tokens” for accessing the Hub 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 the Hub. You must accept the terms and conditions to use the Hub.

## New Features in Version 4.2.0

### License Management

The Hub 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 the Hub. 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 the Hub. 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

The Hub 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

The Hub 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

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

## Ability to Configure Hub 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

The Hub now supports the ability to supply Identity Provider metadata using an xml file.

## New Features in Version 4.1.0

### Kubernetes Support

The Hub 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 the Hub. 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

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

### Remediation Guidance - BETA

A new Beta feature is available in the Hub. For components in your BOM that have vulnerabilities, the Hub 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

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

## SAML for Single Sign-On Support

The Hub now supports the Security Assertion Markup Language (SAML) authentication protocol which enables Multi-Factor Authentication (MFA), 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 Hub Docker Architecture

The new architecture for the Hub is now available. This new architecture consists of "dockerizing" the Hub 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 the Hub as a new installation or upgrade from a previous version, comprised of the old architecture.

Hub 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 Hub 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 Hub-JIRA plugin (version 3.3.0 and higher).

# New Features in Version 3.6.0

## Beta for the New Hub Docker Architecture

A Beta version of the new architecture for the Hub is now available. This new architecture consists of

"dockerizing" the Hub so that different components are containerized which allows other orchestration tools, such as Compose, to manage all of the individual containers.

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

Hub 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-3.6.0.tar>

To get this archive, you can:

```
$ wget https://github.com/blackducksoftware/hub/raw/master/archives/hub-docker-3.6.0.tar
```

Contact Customer Support for any issues.

## Report Database

A PostgreSQL reporting database, `bds_hub_report`, is now available. This database, created automatically when you install or upgrade the Hub, provides access to the following Hub data for reporting purposes:

- Project
- Project version
- Component version
- Component license

## Output the BOM Display to a PDF File

You can output the BOM displayed in the UI as a PDF document. The PDF file displays the BOM similar to what is shown in the UI: security, license, and operational risk graphs appear at the top of the page; component and subproject information is listed in a table.

You can filter the BOM prior to printing so that the PDF file only includes the data you wish to view.

## Ability to add projects to a BOM

If you have projects that are used by other applications, you can now add those projects to a BOM so that the BOM accurately reflects the elements in your application. Adding projects to your application's BOM gives you a complete view of this application and all associated risks, including vulnerabilities, license, and operational risk.

## Dockerized Scan Client

A new script, `scan.docker.sh` is now available for you to use if you are running Docker and have a Docker image that you wish to scan.

The script is bundled with the Hub Scanner. To obtain it, from the Hub UI, select the operating system in the **Hub Scanner** section of the Tools page, download the installer, and unzip the file. The `scan.docker.sh` script is located in the `bin` directory.



**Note:** This script is not available for Windows.

The script creates a .tar archive of the image, uses the Hub Scanner to scan the image, uploads the scan to the Hub, then deletes the tar archive.

To run the script:

```
./scan.docker.sh --image <imagename:version> Hub Scanner command line parameters
```

The image version is optional. Refer to the Hub Scanner help for more information on the command line parameters.

For example:

```
./scan.docker.sh --image jetty:9.3.11-jre8-alpine --username sysadmin --host hostname --port 443 --scheme https
```

Note that Docker needs to be on the PATH.

**Note:** Users running the script must be in the Docker group (best practice) or be root user or have sudo access.

## New Features in Version 3.5

### Adding Comments to a BOM

You can now add comments to a specific component version in a BOM. For example, you can use comments to explain why a component version was ignored or why a policy violation was overridden.

### Review Flags in a BOM

Any user that can edit a BOM can now flag component versions in a BOM as reviewed. Use this feature to indicate that a component version is correctly included in the BOM.

### Code Location Names

The Hub Scanner now supports providing a unique name (alias) to a code location instead of using the host and scan path. This lets you combine multiple host/path combinations into one logical code location.

### Viewing Discovery Source

The Hub now provides the ability to review discoveries from build monitoring plugins such as Maven/Gradle, or from package managers, such as RubyGems. This information appears on the **Source** tab, previously called the **Files** tab.

### Support for Oracle Enterprise Linux 7

The Hub now supports the Oracle Enterprise Linux version 7 operating system.

## New Features in Version 3.4.2

### Hub Email Extension

A Hub email extension that provides the ability to send emails based on notifications from the Hub is now available from the GitHub website (<https://github.com/blackducksoftware/hub-email-extension>).

### New Hub Integration

A Hub integration plugin for Artifactory (version 1.0.1-RC) is now available from the GitHub website (<https://github.com/blackducksoftware/integration-all/>). This plugin enables you to run a component scan and create projects in the Black Duck Hub through an Artifactory job.

## New Features in Version 3.4

This release introduces the following features and functionality.

### New OSS Attribution Module

A new module, the OSS Attribution module, has been added to the Hub. This module allows you to edit and maintain the data needed to create accurate and compliant open source notice files/reports at a project/release level. The notice files can then be included with the distribution or incorporated into documentation to satisfy the attribution obligation.

With the OSS Attribution module, you can make these modifications to the Notices File report:

- Exclude component versions
- Add attribution statements
- Edit license text

### Package Manager Support

The Hub Scanner now supports these package managers:

- RubyGems
- npm

### Better Matching for Linux Distributions

Black Duck has enhanced the matching capabilities when working with Linux distributions by adding package components of CentOS.

## New Features in Version 3.3.2

This release introduces the following feature.

### Ability to Access the REST APIs from a Web Page Served from a non-Hub Server

New properties have been added to the Hub that enable access to the REST APIs from a web page served from a non-Hub server.

## New Features in Version 3.3.1

This release introduces the following features and functionality.

### Extension Support

The Hub now supports external extensions.

Use the new administrative UI in the Hub to add and optionally, configure global and user settings for external extensions for use with the Hub.

### Code Size Limit Notification

The Hub will now notify you when you are approaching your code size limit (as declared in your license). A notification appears in the UI when you are at 80% or higher of your code size limit.

### API Enhancement

A set of vulnerability APIs are now available. Use these APIs to find vulnerabilities by component, component version, component version and origin, and to find a specific vulnerability record.

## New Features in Version 3.3.0

This release introduces the following features and functionality.

### Notices File Report

The Notices File report provides a list of OSS components, versions, and the associated license text. You can use this report to create an attribution report for your project release or to share BOM and license information.

This report is available as a text file or in HTML format.

### Feedback Service

To improve and refine the Black Duck KnowledgeBase (KB) capabilities, a feedback service has been instituted that provides a mechanism to automatically collect BOM adjustments including changes to component name, version, origin, origin ID, or license, for the purpose of improving future matches.

**Note:** No customer-identifiable information is transmitted to the KB.

The feedback service is enabled by default. You can disable this service.

### Support for Maven and Gradle Projects

The Hub now supports dependency BOMs created via the Maven and Gradle Hub plugins.

### API Enhancements

Linked data, role, user group and user role APIs are now available.

### Operating System Support

Support has been added for the following operating systems:

- CentOS 6.8.x
- Ubuntu 16.04.x

## Hub Integrations

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

- Hub Atlassian Config version 1.0.1 and later
- Hub Gradle Plugin version 2.0.6 and later
- Hub Maven Plugin version 1.0.3 and later

## New Features in Version 3.2.0

This release introduces the following features and functionality.

### Subcomponent Discovery

The Hub extends its scanning capability by adding the ability to discover subcomponents contained within open source components in use. For example, Struts (top-level parent component) uses commons.collections (second-level component) which includes commons.io (third-level component).

The BOM includes the complete flat list of all components, including these subcomponents. Risks shown for a BOM include the vulnerabilities for all subcomponents.

### Ability to View Files Affected by a Vulnerability

You can now view the files in a project that are affected by a vulnerability. In the Vulnerability Details page, select the **View related files** option which opens the **Files** tab filtered to display the files affected by this vulnerability.

## Hub Integrations

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

- Bamboo Plugin version 2.0.0 and later
- TFS Plugin version 0.1.0 and later

### Changed Features in 4.5.1

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

### Changed Features in 4.5.0

#### Expanded User Roles

Hub 4.5.1 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 Hub 4.5.1 adds a new Docker container. This provides additional resources, and hands off the authentication.

### Changed Features in 4.4.2

Hub 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 Hub Scan Client

The Hub 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

The Hub 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 the Hub has been increased from 4 to 5 CPUs.

### Dependency Detection Optional in Hub Scanner

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

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

### SAML Enhancement

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

### Column renamed in Project Version Report

Prior to Hub 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.

## Hub Integrations

Go to the GitHub website (<https://github.com/blackducksoftware/integration-all/>) to view available Hub 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 Hub 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 the Hub 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 the Hub using Docker Swarm*
- *Installing the Hub using Docker Compose*
- *Installing the Hub using Kubernetes*

## Japanese Language

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

## Hub Integrations

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

## Tools Page Reorganization

The Tools page has been reorganized:

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

## Improved Usability

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



## Changed Features in 4.2.0

### PostgreSQL version

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

If you are upgrading from a previous version of the Hub, 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 the Hub UI to manage the certificate exchange between the LDAP server and the Hub.

### 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 the Hub.

### Hub Integrations

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

- Hub Artifactory Plugin
- Hub Bamboo Plugin
- Hub Gradle Plugin
- Hub Eclipse Plugin
- Hub Jenkins Plugin
- Hub JIRA Plugin
- Hub Maven Plugin

- Hub NuGet Plugin
- Hub PIP Plugin
- Hub SBT Plugin
- Hub Team City Plugin
- Hub Team City Foundation Server Plugin
- Hub Visual Studio Plugin
- Hub Email Extension
- Hub Docker Inspector
- Hub Detect

**Note:** For complete information on Hub 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 the Hub to increase consistency across the application and make it easier to use.

## Changed Features in 4.1.2

### Logging out of the Hub

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

## Changed Features in 4.1.0

### New Hub Scanner 2.0 - BETA

A Beta version of the Hub Scanner - 2.0 is now available from the Tools page of the Hub 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 the Hub is now managed in a container which will enable faster updates to the documentation.

## LDAP logging

The Hub log files now indicate if LDAP is enabled or disabled.

## PostgreSQL version

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

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

## Hub Integrations

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

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

**Note:** For complete information on Hub 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, the Hub now displays and reports on the actual license

text for licenses which are typically modified for each OSS component. Currently, the Hub 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 Hub 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.

## Hub 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 the Hub 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

The Hub 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.

## Hub Integrations

New versions of the following Hub 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 the Hub 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.

## Hub Integrations

New versions of the following Hub 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 the Hub to increase consistency across the application and make it easier to use.

# Changed Features in 3.6.1

## Hub Integrations

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

- Artifactory Plugin version 2.1.0 and later
- Bamboo Plugin version 3.0.0 and later
- Gradle Plugin version 4.0.0 and later
- JIRA Plugin version 3.2.0 and later
- Maven Plugin version 2.0.0 and later
- TFS Plugin version 2.1.0 and later

# Changed Features in 3.6.0

## Severity Level Added to Policies

You can now add a severity level to a policy. Possible values are: Trivial, Minor, Major, Critical, or Blocker.

You can use this option with build integrations to indicate what should happen when a policy violation occurs. For example, all policy violations with a severity of Blocker should fail the build.

## Improvements to the Hub Scanner

The command line version of the Hub Scanner has added these parameters:

- **--insecure**. Ignores TLS validation errors, allowing the Hub Scanner to connect to the Hub server.
- **--no-prompt**. Runs the Hub Scanner in non-interactive mode. You can set the new `BD_HUB_NO_PROMPT` environment variable to enable non-interactive mode.

## The Protex BOM Tool

The Protex BOM Tool can now export component and license data only. As of release 3.6.0, this will be the default output of the tool. To include the Protex code tree and match details, use the new **--include-files** parameter.

## Read-only user role

The read-only role was modified so that a user with this role can no longer create projects or access the Code Locations page.

## API Enhancements

The following enhancements were made to the REST APIs:

- Improved the aggregate-bom-rest-server API to find a list of projects for a given component and component version.
- Improved the component-rest-server API to provide dependency data.
- Improved the bom-component-comment-rest-server API to add, edit, and remove a BOM comment for a component, with a component version not needed.
- Improved the license-rest-server API to obtain a list of all licenses.
- Added a new version, V2, of the policy-rule-rest-server API. Improved the policy-rule-rest-server API to create, update, and delete policy rules.
- Added a REST API, search-rest-server, to search the Black Duck KnowledgeBase for a component.
- Added a REST API, url-directory-rest-server, to provide a list of APIs for a given user.

## Hub Integrations

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

- Artifactory Plugin version 2.0.2 and later
- Atlassian Config Plugin version 2.0.0 and later
- Bamboo Plugin version 3.0.0 and later
- Jenkins Plugin version 2.1.1 and later
- JIRA Plugin version 3.1.1 and later
- TeamCity Plugin version 3.0.1 and later
- TFS Plugin version 2.0.0 and later

## Hub Email Extension

A new version (1.1.1) of the Hub email extension that provides the ability to send emails based on notifications from the Hub is now available from the GitHub website (<https://github.com/blackducksoftware/hub-email-extension>).

## Japanese Language

The 3.5.1 version of the UI, online help, and release notes has been localized to Japanese.

## Improved Usability

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

## Changed Features in 3.5

### Improvements to the Hub Scanner

The Hub Scanner GUI now supports excluded directories.

### API Enhancements

The following enhancements were made to the REST APIs:

- Added a REST API, bom-component-comment-rest-server, to add, edit, and remove a BOM comment.
- Added the ability to obtain the origin and origin ID in the response when a component and version are requested via the component-version-rest-server API.
- Added a usage field to the aggregate-bom-rest-server response.
- Users now must have the system administrator role to request global notifications using the APIs.

### Hub Integrations

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

- Artifactory Plugin version 1.2.0 and later
- Gradle Plugin version 3.4.1 and later
- JIRA Plugin version 3.0.2 and later
- Maven Plugin version 1.4.0 and later
- TeamCity Plugin version 2.0.0 and later
- TFS Plugin version 1.0.0 and later

### Hub Email Extension

A new version (1.1.0) of the Hub email extension that provides the ability to send emails based on notifications from the Hub is now available from the GitHub website (<https://github.com/blackducksoftware/hub-email-extension>).

### Japanese Language

The 3.4.1 version of the UI, online help, and release notes has been localized to Japanese.

## Improved Usability

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



## Changed Features in 3.4.2

### API Enhancements

The following enhancements were made to the REST APIs:

- Added a REST API, `composite-code-location-rest-server`, to delete specific or all code locations.
- Added a mapped code locations link to the project/version REST API response.
- Added a REST API, `aggregate-bom-rest-server`, to find BOM components.
- Increased the number of project search results to return up to 500 projects.

### Hub Integrations

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

- Atlassian Config Plugin version 1.1.0 and later
- Bamboo Plugin 2.1.0 and later
- Gradle Plugin version 3.1.0 and later
- Jenkins Plugin version 2.0.0 and later
- JIRA Plugin version 3.0.0 and later
- Maven Plugin version 1.2.0 and later

## Changed Features in 3.4

The following features have changed since the last release.

### Modifications to Notices File Report

Users with the new OSS Attribution module can make these changes to the Notices File Report:

- Omit components from the report.
- Add attribution statements.
- Edit the license text.

### Improvements to the Hub Scanner

- Error messages from the Hub Scanner now provide more information as to the cause and possible solution to the problem.
- The file name of the Hub Scanner GUI has been changed to `scan.GUI.sh`.

### Additional Remediation Status

The Duplicate remediation status has been added to the Hub. This remediation status appears if a CVE is related to any VulnDB: the CVE is shown as a new vulnerability and the VulnDB is shown as a vulnerability with a remediation status of Duplicate.

### Ability to View a User's Groups

System administrators can now use the *User Name* page to view the groups a user belongs to. Users can

now see the groups they belong to by using the My Profile page.

## Scan Size Limits

There is now a limit to the scan size. An error message will appear if you exceed the scan size limit, which is typically 5 GB.

## API Enhancements

- To increase user information, a user-filters-rest-server API was added and enhancements were made to the user-group-rest-server and user-rest-server APIs.
- Sending the username and password as url parameters for logging in is no longer supported. The username and password now needed to be included in the body of the request.

## Retention of Historical Scans

In order to reduce memory requirements, the Hub will now only save the current scan and one backup. This change can be seen in the **Scans** section of the Code Locations *Name* page which lists the scans. Contact Customer Support if you need to save additional backup scans.

## Hub Integrations

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

- Atlassian Config Plugin version 1.0.2 and later
- Bamboo Plugin 2.0.1 and later
- Gradle Plugin version 3.0.0 and later
- Jenkins Plugin version 1.5.4 and later
- Maven Plugin version 1.1.0 and later
- TFS Plugin version 0.4.0 and later

## Improved Usability

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

## Japanese Language

The 3.3.1 version of the UI, online help, and release notes has been localized to Japanese.

## Current KnowledgeBase Statistics

As of version 3.4:

- 2,036,044 unique components
- 2491 unique licenses
- 79,217 actively tracked vulnerabilities
- 530,047,513,237 lines of code

## Changed Features in 3.3.1

The following features have changed since the last release.

### Improvements to the Hub Scanner

The Hub Scanner now provides additional methods to exclude directories from scanning:

- Create an `ignore` file located in the `$HOME/config/blackduck` directory.  
Use this file to list excluded directories, relative to root. This option provides you with the ability to use one location to list all directories that need to be excluded.
- Create individual `.bdignore` files which can be located in any directory.  
Use this file to list the excluded subdirectories in the directory where the `.bdignore` file is located. You must create a `.bdignore` file in each directory that has subdirectories you want to exclude.

Both of these methods can be used from the Hub Scanner GUI and from the command line.

### Notification Enhancements

Notifications have been enhanced to include additional vulnerability content.

The notification API framework has also been extended to include additional vulnerability content, support notifications when vulnerabilities are removed, as well as when vulnerabilities are added or updated outside of Black Duck KB update jobs.

### Additional Operand for Policy Rules

To make it easier to create a policy that causes a violation when an unsupported license is used, the "not equal to" operand has been added to the license condition in the Create Policy Rule dialog box.

### Hub Integrations

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

- Jenkins Plugin version 1.5.3 and later
- TeamCity Plugin version 1.4.2 and later
- Hub Gradle Plugin version 2.0.12 and later
- Hub Maven Plugin version 1.0.4 and later

## Changed Features in 3.3.0

The following features have changed since the last release.

### Additional Conditions for Policy Rules

You can now create policy rules that contain a project name and/or project tag condition.

## Improvements to the Hub Scanner

- The Hub Scanner now provides the ability to exclude a single directory or multiple directories from a scan.

Use the **--exclude** parameter to exclude a single directory or the **--exclude-from** parameter to provide a file which lists the directories to exclude from scanning.

- The Windows download of the Hub Scanner now contains a script, CreateGUIShortcut.vbs, which you can use to create a shortcut to the Hub Scanner on your Windows desktop.

## Additional Usage Types

The Hub has added these usage types:

- **Implementation of Standard.** This usage is intended for cases where you implemented according to a standard. For example, a Java spec request that ships with your project.
- **Separate Work.** This usage is intended for loosely-integrated components. Your work is not derived from the component. To be considered a separate work, your application has its own executables, with no linking between the component and your application. An example is including the free Acrobat PDF Viewer with your distribution media.

Both new usage types have no license risk, regardless of the distribution for the project.

## Improvements to Component Scanning and Identification

In this release, the ability to scan self-expanding archives and .lib file archives has been added.

## Configurable Admin Console

You can now change the password for the admin user for the Hub administration console or reset the password to its original value.

## Japanese Language

The 3.2 version of the UI, online help, and release notes has been localized to Japanese.

## Improved Usability

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

## Changed Features in 3.2.0

The following features have changed since the last release.

## Improvements to the Hub Scanner

- The Windows version of the the Hub Scanner GUI no longer displays the command window when running the Hub Scanner.
- The Hub Scanner has added a new parameter, **context**, which can be used to specify additional URL context. Use this parameter, for example, if the X-Forwarded-Prefix header is being specified in a proxy server/load balancer configuration.

## Improved Usability

Usability improvements have been made to the BOM page and the **Files** tab. Also, the UI for vulnerability notifications has been enhanced to provide additional information.

### Fixed Issues in 4.5.0

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

- Fixed an issue wherein a Hub 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 Hub cluster.
- Fixed an issue wherein the Add Comment text box did not have a focused cursor.
- Fixed an issue wherein running Hub 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 Hub version 4.3.1.
- Fixed an issue wherein hosted Hub 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, the Hub may display a blank page.

### Fixed Issues in 4.4.2

Hub 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 the Hub 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 Hub 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 The Hub 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 Hub reports which displayed an incorrect column title for the component name.
- Fixed an issue whereby the Hub Scanner would fail if its own path contained a space.
- Exclude patterns now work when scanning on Windows.
- The Hub 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.

## Fixed Issues in 3.6.1

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

- The Hub now shows matches for ignored components on the **Sources** tab.
- Fixed an issue whereby vulnerability reports could not be generated for large BOMs.
- Notification filters have been updated.
- Fixed an issue whereby an LDAP user could not log in to the Hub.

## Fixed Issues in 3.6.0

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

- The text in the upgrade script regarding the location of the existing database was reworded to remove confusion.
- Fixed an issue whereby a user with only the Code Scanner role could not run scans.
- Fixed an issue whereby if the original sort order was modified, the project version page would not return to the original sort order after a project version was deleted.
- Fixed an issue with the Hub Scanner where an error was received when scanning a Node.js application.

## Fixed Issues in 3.5.2

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

- Fixed an issue in the Hub configured with an email extension whereby users did not receive emails and could not access user information from the User Management section of the HUB UI.

## Fixed Issues in 3.5

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

- Fixed an issue which occurred when appending a project's version with .0.
- BOM components with multiple licenses are now correctly displayed in the CSV format of project version reports.

## Fixed Issues in 3.4.2

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

- Fixed an issue where building the BOM was very slow.

## Fixed Issues in 3.4

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

- Fixed an issue where building the BOM was very slow.
- Improved the Hub's performance when viewing related files in large projects.
- Selecting the User Count link for a component with an unspecified version no longer displays a 404 status code.
- Fixed an issue with component scans that stayed in a "Request Match Job" or "Building BOM" state.
- Fixed an issue where archived versions of projects could be modified.
- Fixed an issue where proxy settings did not persist during an upgrade of the Hub within Docker.
- Fixed an issue where importing a Protex BOM resulted in a persistent "Saving Scan Data" status.

## Fixed Issues in 3.3.0

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

- The Hub Scanner now supports scanning Smali/Baksmali directories.
- Fixed an issue which occurred when registering the Hub through a proxy server.
- When upgrading the Hub, improved reporting of the "Deploy is COMPLETE" message in conjunction with completion of startup background processes.


## Fixed Issues in 3.2.0

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

- Fixed a data migration issue which occurred when upgrading the Hub.

## Chapter 4: Known Issues and Limitations

The following is a list of known issues and limitations in the Hub:

- Searching for a project by name in the Hub may not display any results. To resolve this issue:
  1. Log in to the Hub 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:
  - The Hub supports a single LDAP server. Multiple servers are not supported.
  - If a user is removed from the directory server, the Hub 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, the Hub group is not removed. Delete the group manually.
- Tagging only supports letters, numbers, and the plus (+) and underscore (\_) characters.
- If the Hub 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.