



Release Notes

Version 2021.10.4

A decorative header featuring a complex geometric pattern of overlapping triangles in various shades of teal and blue.

This edition of the *Release Notes* refers to version 2021.10.4 of Black Duck.

This document was created or updated on Friday, January 14, 2022.

Please send your comments and suggestions to:

Synopsys
800 District Avenue, Suite 201
Burlington, MA 01803-5061 USA

Copyright © 2021 by Synopsys.

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.

Chapter 1: Product Announcements	1
Announcements for Version 2021.10.4	1
Security Advisory for Apache Log4J2 (CVE-2021-44832)	1
Announcements for Version 2021.10.3	1
Security Advisory for Apache Log4J2 (CVE-2021-45046 and CVE-2021-45105)	1
Announcements for Version 2021.10.2	2
Security Advisory for Apache Log4J2 (CVE-2021-44228)	2
Announcements for Version 2021.10.0	2
Enhanced Signature Scanning	2
Clarification on Detect 7.4 with Black Duck 2021.8.0	2
PostgreSQL container migration from 9.6 to 11	2
Black Duck PostgreSQL 9.6 deprecation	2
PostgreSQL support schedule	2
Database bds_hub_report deprecation starting with 2021.10.0	3
Upcoming max page limit enforcement for API requests	3
Deprecated APIs	3
Japanese language	4
Simplified Chinese language	4
Announcements for Version 2021.8.0	4
Detect 7.4 required for Black Duck 2021.8.0 release	4
Desktop Scanner on CentOS-7	4
Japanese language	4
Simplified Chinese language	4
Deprecated APIs	4
Announcements for Version 2021.6.0	5
Support ending for PostgreSQL version 9.6 for external databases	5
Deprecated page	5
Deprecated APIs	5
Japanese language	5
Announcements for Version 2021.4.0	5
New containers and changes to system requirements	5
Retention period for unmapped code locations	6
Deprecated APIs	6

New job implementation in 2021.6.0 release	6
Japanese language	7
Announcements for Version 2021.2.0	7
Notice for Azure customers	7
Deprecation of PostgreSQL version 9.6 for external databases	7
Internet Explorer 11 no longer supported	7
Deprecated page	8
Japanese language	8
Announcements for Version 2020.12.0	8
New containers and changes to system requirements	8
Ending support for Internet Explorer 11	8
Japanese language	8
Announcements for Version 2020.10.0	8
New containers and changes to system requirements postponed to the 2020.12.0 release	8
Japanese language	9
Announcement for Version 2020.8.0	9
Deprecation of PostgreSQL version 9.6 for external databases	9
Deprecated API in 2020.10.0 release	9
Japanese language	9
Announcement for Version 2020.6.1	10
Ending support for Internet Explorer 11	10
Announcement for Version 2020.6.0	10
New containers and changes to system requirements in future releases	10
Deprecating Internet Explorer 11 support	11
PostgreSQL 11 support for external databases	11
Announcement for Version 2020.2.0	11
Individual file matching	11
Docker Compose support	12
Chapter 2: Release Information	13
Version 2021.10.4	13
New and Changed Features in Version 2021.10.4	13
Fixed Issues in 2021.10.4	14
Version 2021.10.3	14
New and Changed Features in Version 2021.10.3	14
Fixed Issues in 2021.10.3	15
Version 2021.10.2	15
New and Changed Features in Version 2021.10.2	15
Fixed Issues in 2021.10.2	15
Version 2021.10.1	16
New and Changed Features in Version 2021.10.1	16
Fixed Issues in 2021.10.1	16

Version 2021.10.0	17
New and Changed Features in Version 2021.10.0	17
API Enhancements	19
Fixed Issues in 2021.10.0	21
Version 2021.8.5	22
New and Changed Features in Version 2021.8.5	22
Fixed Issues in 2021.8.5	22
Version 2021.8.4	23
New and Changed Features in Version 2021.8.4	23
Fixed Issues in 2021.8.4	23
Version 2021.8.3	24
New and Changed Features in Version 2021.8.3	24
Fixed Issues in 2021.8.3	24
Version 2021.8.2	25
New and Changed Features in Version 2021.8.2	25
Fixed Issues in 2021.8.2	25
Version 2021.8.1	25
New and Changed Features in Version 2021.8.1	25
Fixed Issues in 2021.8.1	26
Version 2021.8.0	26
New and Changed Features in Version 2021.8.0	26
Fixed Issues in 2021.8.0	31
Version 2021.6.2	32
New and Changed Features in Version 2021.6.2	32
Fixed Issues in 2021.6.2	32
Version 2021.6.1	32
New and Changed Features in Version 2021.6.1	32
Fixed Issues in 2021.6.1	33
Version 2021.6.0	34
New and Changed Features in Version 2021.6.0	34
Fixed Issues in 2021.6.0	39
Version 2021.4.1	40
New and Changed Features in Version 2021.4.1	40
Fixed Issues in 2021.4.1	40
Version 2021.4.0	40
New and Changed Features in Version 2021.4.0	40
Fixed Issues in 2021.4.0	45
Version 2021.2.1	47
New and Changed Features in Version 2021.2.1	47
Fixed Issues in 2021.2.1	47
Version 2021.2.0	48

New and Changed Features in Version 2021.2.0	48
Fixed Issues in 2021.2.0	53
Version 2020.12.0	54
New and Changed Features in Version 2020.12.0	54
Fixed Issues in 2020.12.0	59
Version 2020.10.1	60
New and Changed Features in Version 2020.10.1	60
Fixed Issues in 2020.10.1	60
Version 2020.10.0	60
New and Changed Features in Version 2020.10.0	60
Fixed Issues in 2020.10.0	66
Chapter 3: Known Issues and Limitations	68
New Known Issues	68
Current Known Issues and Limitations	68

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 Swarm	install_swarm.pdf	Contains information about installing and upgrading Black Duck using Docker Swarm.
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.
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.

The installation methods for installing Black Duck software in a Kubernetes or OpenShift environment are Synopsysctl and Helm. Click the following links to view the documentation.

- [Helm](#) is a package manager for Kubernetes that you can use to install Black Duck.
- [Synopsysctl](#) is a cloud-native administration command-line tool for deploying Black Duck software in Kubernetes and Red Hat [OpenShift](#).

Black Duck integration documentation is available on [Confluence](#).

Customer support

If you have any problems with the software or the documentation, please contact Synopsys Customer Support.

You can contact Synopsys Support in several ways:

- Online: <https://www.synopsys.com/software-integrity/support.html>
- Phone: See the Contact Us section at the bottom of our [support page](#) to find your local phone number.

To open a support case, please log in to the Synopsys Software Integrity Community site at <https://community.synopsys.com/s/contactsupport>.

Another convenient resource available at all times is the [online customer portal](#).

Synopsys Software Integrity Community

The Synopsys Software Integrity Community is our primary online resource for customer support, solutions, and information. The 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 Software Integrity Group (SIG) customers. The many features included in the 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 SIG 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 Synopsys 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 SIG experts and our Knowledgebase.
- Share - Collaborate and connect with Software Integrity Group 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, click [here](#) to get started, or send an email to community.manager@synopsys.com.

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://community.synopsys.com/s/education> or for help with Black Duck, select **Black Duck**

Tutorials from the Help menu () in the Black Duck UI.

Synopsys Statement on Inclusivity and Diversity

Synopsys is committed to creating an inclusive environment where every employee, customer, and partner feels welcomed. We are reviewing and removing exclusionary language from our products and supporting customer-facing collateral. Our effort also includes internal initiatives to remove biased language from our engineering and working environment, including terms that are embedded in our software and IPs. At the same time, we are working to ensure that our web content and software applications are usable to people of varying abilities. You may still find examples of non-inclusive language in our software or documentation as our IPs implement industry-standard specifications that are currently under review to remove exclusionary language.

Chapter 1: Product Announcements

Announcements for Version 2021.10.4

Security Advisory for Apache Log4J2 (CVE-2021-44832)

The Apache Organization released a new version (2.17.1) of the Log4j2 component, which addresses a new vulnerability.

Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.

For more information, see the [official CVE posting](#) and [Apache's Log4j Security Vulnerabilities page](#).

As stated with the Black Duck 2021.10.3 version, we believe that there is limited exposure to Synopsys' products, services and systems. To the extent we have had exposure, we have remediated or are in the process of remediating the situation. Please continue monitoring our [community page](#) for further updates.

Announcements for Version 2021.10.3

Security Advisory for Apache Log4J2 (CVE-2021-45046 and CVE-2021-45105)

The Apache Organization released a new version (2.17.0) of the Log4j2 component, which addresses an additional vulnerability not fixed in versions 2.15.0 and 2.16.0.

[CVE-2021-45046](#) allows attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup or a Thread Context Map pattern to craft malicious input data using a JNDI Lookup pattern resulting in a denial of service (DOS) attack.

[CVE-2021-45105](#) allows attackers with control over Thread Context Map (MDC) input data to craft malicious input data that contains a recursive lookup, resulting in a StackOverflowError that will terminate the process resulting in a denial of service (DOS) attack.

For more information, see [Apache's Log4j Security Vulnerabilities page](#).

As stated with the Black Duck 2021.10.2 version, we believe that there is limited exposure to Synopsys' products, services and systems. To the extent we have had exposure, we have remediated or are in the process of remediating the situation. Please continue monitoring our [community page](#) for further updates.

Announcements for Version 2021.10.2

Security Advisory for Apache Log4J2 (CVE-2021-44228)

Synopsys is aware of the security issue relating to the open-source Apache Log4j 2 Java library dubbed Log4Shell (or LogJam) which was disclosed publicly via the project's GitHub on December 9, 2021. The vulnerability allows for unauthenticated remote code execution and impacts Apache Log4j 2 versions 2.0 to 2.14.1. For more information, see the [official CVE posting](#).

Based on what we know at this time, we believe that there is limited exposure to Synopsys' products, services and systems. To the extent we have had exposure, we have remediated or are in the process of remediating the situation. Please continue monitoring our [community page](#) for further updates.

See also: <https://www.synopsys.com/blogs/software-security/zero-day-exploit-log4j-analysis/>

Announcements for Version 2021.10.0

Enhanced Signature Scanning

The same performance improvements that were introduced to Package Manager Scanning in the 2021.8.0 release are available in the 2021.10.0 release for Signature Scanning. A key part of these improvements is Duplicate BOM Detection. With this feature, if a Signature Scan will not alter the BOM already associated with the specific Project and Version, then BOM Computation is bypassed.

Additionally, with Enhanced Signature Scanning the JobRunner no longer plays a role in processing of incoming Package Manager or Signature Scans. Although more system resources are not required to run Enhanced Signature Scans, it is possible that minor rebalancing of the containers is required. Please reach out to Synopsys support who can help you understand if any rebalancing is needed. We encourage all our customers to do so and take advantage of these improved capabilities.

Clarification on Detect 7.4 with Black Duck 2021.8.0

In order to ensure full functionality and compatibility, Black Duck version 2021.8.0 requires Detect 7.4. Users can continue to use older versions of Detect with Black Duck, but may encounter inaccurate dependency types or source views in the BOM when using aggregated BDIO files.

Upgrading to Detect 7.4 will ensure you avoid these inaccuracies in the BOM.

PostgreSQL container migration from 9.6 to 11

Black Duck will migrate its PostgreSQL image from version 9.6 to version 11 with the **2022.2.0** release. Customers not using the Synopsys-supplied PostgreSQL image will not be affected.

Black Duck PostgreSQL 9.6 deprecation

As announced in the Black Duck 2020.6.0 release, Black Duck was to end support for external PostgreSQL 9.6 for the 2021.6.0 release. Starting with the **2022.2.0** release, Black Duck will no longer work with PostgreSQL 9.6 and will fail to start if pointed to a PostgreSQL 9.6 instance.

PostgreSQL support schedule

Starting with the upcoming **2022.10.0** release, Black Duck will end support for external PostgreSQL 11.

Please see the table below for the projected dates for the beginning and end of support for future PostgreSQL versions.

PG Version	First Release	Last Release	BD External Support Added	BD External Support End
16.x	Late 2023	Late 2028	2024.10.0	2026.10.0
15.x	Late 2022	Late 2027	2023.10.0	2025.10.0
14.x	September 2021	November 2026	2022.10.0	2024.10.0
13.x	September 2020	November 2025	2021.8.0	2023.10.0
12.x	October 2019	November 2024	X	X
11.x	October 2018	November 2023	2020.6.0	2022.10.0

Database `bds_hub_report` deprecation starting with 2021.10.0

Starting with 2021.10.0, new installations of Black Duck will no longer create the `bds_hub_report` database. We plan to finally delete `bds_hub_report` in 2022.10.0.

Also, the `hub_create_data_dump.sh` and `hub_db_migrate.sh` scripts (which are distributed with our orchestration files) will no longer fail if `bds_hub_report` does not exist.

- The `hub_create_data_dump.sh` script will dump `bds_hub_report` if it exists but will not fail if it doesn't. If `bds_hub_report` is absent, the script will print a message saying it was skipped.
- The `hub_db_migrate.sh` script will try to restore `bds_hub_report` if it exists, regardless of whether or not a dump file is present (matching the behavior of prior releases). If `bds_hub_report` is not present, it will not try to restore it, also regardless of whether or not a dump file is present.
- A new script, `hub_recreate_reportdb.sh` is added to recreate `bds_hub_report` if a user wants propagate their `bds_hub_report` DBs from 2021.8.x or earlier to a new install of 2021.10.0 or later. In this case;
 - Run `hub_create_data_dump.sh` on the old BD instance.
 - Run `hub_recreate_reportdb.sh` on the new BD instance.
 - Run `hub_db_migrate.sh` on the new BD instance with the dumps created in step #1.

Upcoming max page limit enforcement for API requests

Starting with Black Duck **2022.2.0**, max page limits on API requests will be enforced. Users should make singular requests that include a limit request parameter smaller or equal to the documented page limit. Requests for pages greater than the documented limit will be truncated to only return the maximum accepted page limit. Requests for page sizes will not be rejected but return a maximum number of results per paged request.

This will be an ongoing effort lasting subsequent releases to improve application stability and prevent performance degradation from unreasonably large requests.

Deprecated APIs

The following defunct endpoints will now return a 404 NOT FOUND error to indicate that access to the target resource is no longer available:

- GET /oauthclients
- POST /oauthclients
- DELETE /oauthclients/{oAuthClientId}
- GET /oauthclients/{oAuthClientId}
- PUT /oauthclients/{oAuthClientId}
- POST /vulnerabilities/vulndb-copy

Japanese language

The 2021.8.0 version of the UI, online help, and release notes has been localized to Japanese.

Simplified Chinese language

The 2021.8.0 version of the UI, online help, and release notes has been localized to Simplified Chinese.

Announcements for Version 2021.8.0

Detect 7.4 required for Black Duck 2021.8.0 release

Black Duck version 2021.8.0 requires Detect 7.4 in order to run. Please ensure you meet this minimum version requirement when upgrading.

Desktop Scanner on CentOS-7

As a result of updated dependencies, the latest version of Desktop Scanner will not run on CentOS-7. Therefore, a different RPM was created specifically for the CentOS-7 build which will be running with an older version of Electron 12. We will maintain this separate CentOS-7 build for as long as Electron 12 is supported.

In addition to our current downloads, a link has been added on the Tools page specifically for the CentOS-7 download. The regular RPM, debian package, macOS and Windows installers are available as usual.

Japanese language

The 2021.6.0 version of the UI, online help, and release notes has been localized to Japanese.

Simplified Chinese language

The 2021.2.0 version of the UI, online help, and release notes has been localized to Simplified Chinese.

Deprecated APIs

The following endpoint has been removed:

- GET /api/scan/{scanId}/bom-entries

The following defunct endpoints will now return a 410 GONE error to indicate that access to the target resource is no longer available:

- GET /oauthclients
- POST /oauthclients

- DELETE /oauthclients/{oAuthClientId}
- GET /oauthclients/{oAuthClientId}
- PUT /oauthclients/{oAuthClientId}
- POST /vulnerabilities/vulndb-copy

Announcements for Version 2021.6.0

Support ending for PostgreSQL version 9.6 for external databases

As of the Black Duck 2021.6.0 release, Synopsys has ended support for PostgreSQL version 9.6 for external databases.

Black Duck will now only support PostgreSQL version 11.x for external databases.

Deprecated page

As announced previously, the Scans > Components page has been removed.

Deprecated APIs

The following endpoints have been deprecated:

- GET /oauthclients
- POST /oauthclients
- DELETE /oauthclients/{oAuthClientId}
- GET /oauthclients/{oAuthClientId}
- PUT /oauthclients/{oAuthClientId}
- POST /vulnerabilities/vulndb-copy

Japanese language

The 2021.4.0 version of the UI, online help, and release notes has been localized to Japanese.

Announcements for Version 2021.4.0

New containers and changes to system requirements

In the 2021.6.0 release:

- A new container, blackduck-webui, will be added for improved Black Duck performance, better caching, and future scalability.
- The Rapid Scanning feature will be available to all Black Duck customers. This feature requires a new container, currently called blackduck-kb, which will manage connections to the Black Duck KnowledgeBase and cache KnowledgeBase results for short intervals.

The following will be the minimum hardware that will be needed to run a single instance of all containers. Note that memory requirements depend on the number of concurrent Rapid Scans you want to support.

- 7 CPUs
- 28.5 GB RAM for the minimum Redis configuration; 31.5 GB RAM for an optimal configuration providing higher availability for Redis-driven caching. This will support up to 100 concurrent Rapid Scans.

30 GB RAM for the minimum Redis configuration; 33 GB RAM for an optimal configuration providing higher availability for Redis-driven caching. This will support more than 150 Rapid Scans, however, the maximum number of supported Rapid Scans is still being determined.

- 250 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

The following is the minimum hardware that is needed to run Black Duck with Black Duck - Binary Analysis.

- 8 CPUs
- 32.5 GB RAM for the minimum Redis configuration; 35.5 GB RAM for an optimal configuration providing higher availability for Redis-driven caching. This will support up to 100 concurrent Rapid Scans.

34 GB RAM for the minimum Redis configuration; 37 GB RAM for an optimal configuration providing higher availability for Redis-driven caching. This will support more than 150 Rapid Scans, however, the maximum number of supported Rapid Scans is still being determined.

- 350 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

Note: An additional CPU, 2 GB RAM, and 100 GB of free disk space will be needed for every additional binaryscanner container.

Retention period for unmapped code locations

In the Black Duck 2021.6.0 release, the default retention period for unmapped code locations will be changing from 365 days to 30 days.

Deprecated APIs

The following endpoint has been deprecated and will be removed in a future release:

```
GET /api/scan/{scanId}/bom-entries
```

The following endpoint will be deprecated as of April 30, 2021:

```
GET /api/components/{componentId}/versions/{componentVersionId}/origins/{originId}/direct-dependencies
```

New job implementation in 2021.6.0 release

In the Black Duck version 2021.6.0, the jobs subsystem is being replaced with a new implementation, which will cause the following job Rest API calls not to function.

- GET /jobs/{jobID}

This call gets the job details for a specific job by ID. As of the Black Duck 2021.6.0 release, this call will return a 404 Not Found status code.

The following calls are out-of-service since Black Duck version 2020.2.0, returning a 404 Not Found status code, and will remain non-functional in Black Duck version 2021.6.0.

- PUT /jobs/{jobID}

This call reschedules a job.

- DELETE /jobs/{jobID}

This call terminates a job.

The functionality will be replaced with a new Job Rest API implementation which will be available in a future release.

Japanese language

The 2021.2.0 version of the UI, online help, and release notes has been localized to Japanese.

Announcements for Version 2021.2.0

Notice for Azure customers

Black Duck version 2021.2.0 is being released with a known issue which impacts customers who deploy on Azure Kubernetes Services (AKS) and use Azure Database for PostgreSQL as an external database. Please note, this is the standard, recommended configuration for Black Duck customers on the Azure platform. At this time, it is NOT recommended that customers running on the Azure platform with an external database upgrade to 2021.2.0. Doing so will leave your system inoperable and force you to restore your installation back to the prior state.

We expect this to be resolved in a future release of Black Duck and will make the announcement when the release details are known.

If you are running on AKS and use an internal PostgreSQL database, there is no issue and the system works as expected. However, this would be an atypical installation on the AKS platform.

If you have concerns and questions, please reach out to Black Duck support for assistance.

Deprecation of PostgreSQL version 9.6 for external databases

Synopsys will be ending support for PostgreSQL version 9.6 for external databases starting with the Black Duck 2021.6.0 release.

As of the Black Duck 2021.6.0 release, Black Duck will only support PostgreSQL version 11.x for external databases.

Internet Explorer 11 no longer supported

Synopsys has ended support for Internet Explorer 11.

Deprecated page

The Scans > Components page is deprecated as of the 2021.2.0 release and will be removed in a future release.

Japanese language

The 2020.12.0 version of the UI, online help, and release notes has been localized to Japanese.

Announcements for Version 2020.12.0

New containers and changes to system requirements

There are two additional containers: BOM Engine and RabbitMQ (now a required container) for the 2020.12.0 release.

The minimum system requirements to run a single instance of all containers are:

- 6 CPUs
- 26 GB RAM for the minimum Redis configuration; 29 GB RAM for an optimal configuration providing higher availability for Redis-driven caching
- 250 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

The minimum hardware that is needed to run Black Duck with Black Duck - Binary Analysis are:

- 7 CPUs
- 30 GB RAM for the minimum Redis configuration; 33 GB RAM for an optimal configuration providing higher availability for Redis-driven caching
- 350 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

Note: An additional CPU, 2 GB RAM, and 100 GB of free disk space will be needed for every additional binaryscanner container.

Ending support for Internet Explorer 11

Support for Internet Explorer 11 is deprecated and Synopsys will be ending support for Internet Explorer 11 starting with the Black Duck 2021.2.0 release.

Japanese language

The 2020.10.0 version of the UI, online help, and release notes has been localized to Japanese.

Announcements for Version 2020.10.0

New containers and changes to system requirements postponed to the 2020.12.0 release

Black Duck had announced previously that there would be two additional containers: BOM Engine and

RabbitMQ (now a required container), for the 2020.10.0 release. This requirement has been postponed to the 2020.12.0 release.

For the 2020.12.0 release, the minimum system requirements to run a single instance of all containers will be:

- 6 CPUs
- 26 GB RAM for the minimum Redis configuration; 29 GB RAM for an optimal configuration providing higher availability for Redis-driven caching
- 250 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

For the 2020.12.0 release, the minimum hardware that is needed to run Black Duck with Black Duck - Binary Analysis will be:

- 7 CPUs
- 30 GB RAM for the minimum Redis configuration; 33 GB RAM for an optimal configuration providing higher availability for Redis-driven caching
- 350 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

Note: An additional CPU, 2 GB RAM, and 100 GB of free disk space will be needed for every additional binaryscanner container.

Japanese language

The 2020.8.0 version of the UI, online help, and release notes has been localized to Japanese.

Announcement for Version 2020.8.0

Deprecation of PostgreSQL version 9.6 for external databases

Synopsys will be deprecating support for PostgreSQL version 9.6 for external databases starting with the Black Duck 2021.6.0 release.

As of the Black Duck 2021.6.0 release, Black Duck will only support PostgreSQL version 11.x for external databases.

Deprecated API in 2020.10.0 release

In the Black Duck 2020.10.0 release, the `/api/catalog-risk-profile-dashboard` API will return HTTP 410 (GONE) and as of the Black Duck 2020.12.0 release, this API will not be available.

A new API to replace `/api/catalog-risk-profile-dashboard` will be announced in the 2020.10.0 release.

Japanese language

The 2020.6.0 version of the UI, online help, and release notes has been localized to Japanese.

Announcement for Version 2020.6.1

Ending support for Internet Explorer 11

Support for Internet Explorer 11 is deprecated and Synopsys will be ending support for Internet Explorer 11 starting with the Black Duck 2021.2.0 release.

Announcement for Version 2020.6.0

New containers and changes to system requirements in future releases

2020.8.0 release

In the **2020.8.0 release**, a new Redis container will be added to Black Duck. This container will enable more consistent caching functionality in Black Duck and will be used to improve application performance.

The following will be the minimum hardware that will be needed to run a single instance of all containers:

- 5 CPUs
- 21 GB RAM for the minimum Redis configuration; 24 GB RAM for an optimal configuration providing higher availability for Redis-driven caching
- 250 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

The following will be the minimum hardware that will be needed to run Black Duck with Black Duck - Binary Analysis:

- 6 CPUs
- 25 GB RAM for the minimum Redis configuration; 28 GB RAM for an optimal configuration providing higher availability for Redis-driven caching
- 350 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

Note: An additional CPU, 2 GB RAM, and 100 GB of free disk space is needed for every additional binaryscanner container.

2020.10.0 release

For the **2020.10.0 release**, Black Duck will be adding two additional containers: BOM Engine and RabbitMQ, which will be a required container. These containers will be used to improve application performance, primarily improving project version BOM performance.

Initial testing indicates that minimum system requirements to run a single instance of all containers will be the following:

- 6 CPUs
- 26 GB RAM for the minimum Redis configuration; 29 GB RAM for an optimal configuration providing higher availability for Redis-driven caching

- 250 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

Initial testing indicates that the minimum hardware that is needed to run Black Duck with Black Duck - Binary Analysis will be the following:

- 7 CPUs
- 30 GB RAM for the minimum Redis configuration; 33 GB RAM for an optimal configuration providing higher availability for Redis-driven caching
- 350 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

Note: An additional CPU, 2 GB RAM, and 100 GB of free disk space is needed for every additional binaryscanner container.

Note that these system requirements are based on initial testing results. Final system requirements may be less than what is indicated here, but will not be more than what is listed here.

Deprecating Internet Explorer 11 support

Synopsys will be deprecating support for Internet Explorer 11 starting with the Black Duck 2021.2.0 release.

PostgreSQL 11 support for external databases

Black Duck now supports PostgreSQL 11.7 for new installs that use external PostgreSQL. While PostgreSQL 9.6 continues to be fully supported for external PostgreSQL instances, Synopsys recommends PostgreSQL 11.7 for new installs that use external PostgreSQL.

For users of the internal PostgreSQL container, PostgreSQL 9.6 remains the supported version for Black Duck 2020.6.0.

Announcement for Version 2020.2.0

Individual file matching

As previously announced, to reduce false positives due to ambiguous matches, performing individual file matching as a part of signature scanning is no longer the default behavior for Black Duck CLI and Synopsys Detect scans.

Individual file matching is the identification of a component based purely upon the checksum information of a single file. In Black Duck, for a small set of file extensions (.js, .apklib, .bin, .dll, .exe, .o, and .so), regular signature scanning matches files to components based upon a checksum match to the one file. Unfortunately, this matching is not always accurate and produced a fair amount of false positives. In order to improve upon the overall developer experience across the broad Synopsys customer base, individual file matching is no longer the default behavior and instead is now an optional capability.

Upgrading to 2020.2.0 will turn individual file matching off and may cause some components to drop off the BOM. To estimate the impacts to your BOM, please look for components with only the match type of "Exact File" to see components that may drop from your BOM. Please note, if you are scanning docker images,

“Exact File” matches are not impacted by this change.

The Signature Scanner has a new parameter to enable individual file matching. if you are using Synopsys Detect to scan, version 6.2 will have a new parameter to support turning on/off individual file matching, with the default being “off”.

Docker Compose support

As announced previously, Docker Compose is no longer a supported orchestration method with the 2020.2.0 release.

Version 2021.10.4

New and Changed Features in Version 2021.10.4

Log4j Update

The Apache Log4j 2 Java library has been updated to 2.17.1 to address the CVE-2021-44832 vulnerability.

Logstash Notice

The Logstash image included in Blackduck still uses Logstash 7.16.2 which has Log4j 2.17.0. This is the latest version of Logstash available at the time of this writing. You can avoid the CVE-2021-44832 vulnerability by ensuring that you do not change your configuration as described in the [vulnerability's details](#).

Logstash Container Memory Increase

Due to potential crashing or restarts caused by out of memory issues, we have increased the memory allocated to the Logstash container from 1024M to 2560M. This should result in fewer webapp interruptions, impacting your operations.

Container versions

- blackducksoftware/blackduck-postgres:9.6-1.4
- blackducksoftware/blackduck-authentication:2021.10.4
- blackducksoftware/blackduck-webapp:2021.10.4
- blackducksoftware/blackduck-scan:2021.10.4
- blackducksoftware/blackduck-jobrunner:2021.10.4
- blackducksoftware/blackduck-cfssl:1.0.4
- blackducksoftware/blackduck-logstash:1.0.15
- blackducksoftware/blackduck-registration:2021.10.4
- blackducksoftware/blackduck-nginx:2.0.9
- blackducksoftware/blackduck-documentation:2021.10.4
- blackducksoftware/blackduck-upload-cache:1.0.19
- blackducksoftware/blackduck-redis:2021.10.4
- blackducksoftware/blackduck-bomengine:2021.10.4
- blackducksoftware/blackduck-matchengine:2021.10.4

- blackducksoftware/blackduck-webui:2021.10.4
- sigsynopsys/bdba-worker:2021.9.2
- blackducksoftware/rabbitmq:1.2.6

Fixed Issues in 2021.10.4

The following issues were fixed in this release:

- (HUB-32142). Fixed an issue where RabbitMQ could fail to install on Openshift as a result of missing permissions.
- (HUB-31964). Fixed an issue where some reports could not be generated due to VersionReportJob failing for a project-version as a result of JDBC having too many parameters.
- (HUB-30088). Fixed an issue whereby the logout page did not appear when logging out of a SSO account.
- (HUB-32031). Fixed an issue where HELM matchengine replicas value were hardcoded in 2021.6 and 2021.8 and 2021.10.

Version 2021.10.3

New and Changed Features in Version 2021.10.3

Log4j Update

The Apache Log4j 2 Java library has been updated to 2.17.0 to address the critical CVE-2021-45046 and CVE-2021-45105 vulnerabilities.

Logstash Update

The Logstash image used in Black Duck has been upgraded to 7.16.2 which uses Log4j2 version 2.17.0.

Container versions

- blackducksoftware/blackduck-postgres:9.6-1.4
- blackducksoftware/blackduck-authentication:2021.10.3
- blackducksoftware/blackduck-webapp:2021.10.3
- blackducksoftware/blackduck-scan:2021.10.3
- blackducksoftware/blackduck-jobrunner:2021.10.3
- blackducksoftware/blackduck-cfssl:1.0.4
- blackducksoftware/blackduck-logstash:1.0.15
- blackducksoftware/blackduck-registration:2021.10.3
- blackducksoftware/blackduck-nginx:2.0.9
- blackducksoftware/blackduck-documentation:2021.10.3
- blackducksoftware/blackduck-upload-cache:1.0.19
- blackducksoftware/blackduck-redis:2021.10.3
- blackducksoftware/blackduck-bomengine:2021.10.3
- blackducksoftware/blackduck-matchengine:2021.10.3

- blackducksoftware/blackduck-webui:2021.10.3
- sigsynopsys/bdba-worker:2021.9.2
- blackducksoftware/rabbitmq:1.2.5

Fixed Issues in 2021.10.3

The following issues were fixed in this release:

- (HUB-32233). Upgraded Log4j to version 2.17.0 in response to CVE-2021-45046 and CVE-2021-45105.
- (HUB-32295). Updated Bitnami Logstash to 7.16.2 version with Log4j 2.17.0.

Version 2021.10.2

New and Changed Features in Version 2021.10.2

Log4j Update

The Apache Log4j 2 Java library has been updated to 2.15.0 to address the critical CVE-2021-44228 vulnerability.

Container versions

- blackducksoftware/blackduck-postgres:9.6-1.4
- blackducksoftware/blackduck-authentication:2021.10.2
- blackducksoftware/blackduck-webapp:2021.10.2
- blackducksoftware/blackduck-scan:2021.10.2
- blackducksoftware/blackduck-jobrunner:2021.10.2
- blackducksoftware/blackduck-cfssl:1.0.4
- blackducksoftware/blackduck-logstash:1.0.13
- blackducksoftware/blackduck-registration:2021.10.2
- blackducksoftware/blackduck-nginx:2.0.9
- blackducksoftware/blackduck-documentation:2021.10.2
- blackducksoftware/blackduck-upload-cache:1.0.19
- blackducksoftware/blackduck-redis:2021.10.2
- blackducksoftware/blackduck-bomengine:2021.10.2
- blackducksoftware/blackduck-matchengine:2021.10.2
- blackducksoftware/blackduck-webui:2021.10.2
- sigsynopsys/bdba-worker:2021.9.2
- blackducksoftware/rabbitmq:1.2.5

Fixed Issues in 2021.10.2

The following issue was fixed in this release:

- (HUB-32174). Upgraded Log4j to version 2.15.0 in response to CVE-2021-44228.

Version 2021.10.1

New and Changed Features in Version 2021.10.1

RestResponseErrorHandler Improvement

RestResponseErrorHandler now more gracefully accommodates unexpected responses from the KnowledgeBase and other servers within the network to improve the reliability of Black Duck features.

Container versions

- blackducksoftware/blackduck-postgres:9.6-1.4
- blackducksoftware/blackduck-authentication:2021.10.1
- blackducksoftware/blackduck-webapp:2021.10.1
- blackducksoftware/blackduck-scan:2021.10.1
- blackducksoftware/blackduck-jobrunner:2021.10.1
- blackducksoftware/blackduck-cfssl:1.0.4
- blackducksoftware/blackduck-logstash:1.0.11
- blackducksoftware/blackduck-registration:2021.10.1
- blackducksoftware/blackduck-nginx:2.0.9
- blackducksoftware/blackduck-documentation:2021.10.1
- blackducksoftware/blackduck-upload-cache:1.0.19
- blackducksoftware/blackduck-redis:2021.10.1
- blackducksoftware/blackduck-bomengine:2021.10.1
- blackducksoftware/blackduck-matchengine:2021.10.1
- blackducksoftware/blackduck-webui:2021.10.1
- sigsynopsys/bdba-worker:2021.9.1
- blackducksoftware/rabbitmq:1.2.5

Fixed Issues in 2021.10.1

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

- (HUB-31129). Fixed an issue where project versions reports in the Hub (for example the Vulnerability Detail report) would print out a URL for the vulnerabilities with CVEs containing a BDSA record if the component has a BDSA record as well. The vulnerability reports will now not print the CVE link with the BDSA number appended.
- (HUB-31293). Fixed an issue where Python transitive dependencies were changed to direct dependencies after upgrading to 2021.8.x.
- (HUB-31764). Fixed an issue causing Null Pointer Exceptions during BOM computation when the remediation status of a vulnerability was updated.
- (HUB-30004). Fixed a permission issue in OpenShift environments where successful binary scans using Detect could produce blank BOMs on HUB.

- (HUB-31879). Fixed an issue where scans could get stuck during the building bom phase. See the `RestResponseErrorHandler` improvement in the New and Changed Features section above for more details.
- (HUB-31896). Fixed an issue where remediation updates to BOM vulnerabilities via public api did not persist after re-scan.
- (HUB-31753). Fixed an issue where the `CollectScanStatsJob` job could take longer than expected to complete, leading to unnecessary database bloat.
- (HUB-31663). Fixed an issue where the `QuartzSearchDashboardRefreshJob` could get into a condition where it tried to schedule multiple instances of this job potentially causing a large amount of blocked queries to the database.
- (HUB-31755). Fixed an issue when generating a Project Version report that could cause `VersionReportJob` to run out of memory due to cyclic project structure.
- (HUB-31566). Fixed an issue where services could experience database connection errors due to job over-scheduling, out-of-memory issues, and/or long-running jobs.

Version 2021.10.0

New and Changed Features in Version 2021.10.0

Signature scanner dry run update

Previously, when performing a Signature Scanner dry run, the output would produce a JSON file. Starting with Black Duck 2021.10.0, the produced output file will be a .bdio extension, and is a zip file. It will continue to be generated in the same directory as dry run as traditional signature scanning.

Updated error messages for the Enhanced Signature Generation

Signature scanning server-side error messages have been updated. A complete list of error messages will be made available in the user guide in an upcoming release.

Unmapped scans data retention configuration setting

A new configuration setting is now available for administrators to change the default retention period for unmapped scans. Starting with Black Duck 2021.10.0, this setting will be enabled by default and set to a period of 30 days (previously 365 days). This retention setting can be updated and set to as low as 1 day and to as high as 365 days.



To change this setting in the UI, click , click Settings, and then click Data Retention.

Estimated Security Risk

This estimated risk statistic is formulated by looking at all the versions of a component sorted by security vulnerability severity category and calculating the maximum vulnerability count for each severity category for each component version. The maximum vulnerability count for each severity category is shown in the "Estimated Security Risk by Severity Category" on the Bill of Material for Security risk. The highest severity category counts may reference different component versions. For example:

- Version 1.1 has 2 Critical, 3 High, 15 Medium, 4 Low
- Version 1.2 has 2 Critical, 4 High, 12 Medium, 1 Low
- Estimated Security Risk by severity category for components with unknown versions would return as 2 Critical, 4 High, 15 Medium, 4 Low on the BoM.

Users should choose the exact version used in the application to view the accurate risk instead of the estimated risk. This estimated risk information is provided to help prioritize what components to review first. Users are encouraged to use estimated risk information in conjunction with BD Policy Management to further prioritize what components to triage first based on their company's security policies.

Note: The information presented is only a statistical data estimation. As a result, the estimated security risks will not have CVE data.





Generating Notices report when deep license data is enabled

The notices file will now place any declared licenses before additional ones. The declared and additional licenses will then be sorted alphabetically.


Addition of comments to the Source view and the Source report

Comments can now be added to entries in the Source view of a project. File comments are also shown in the snippet view. These comments also appear in the Source Report in the new column labeled Comments. Select the Source check box for the Version Detail Report in the Report tab to create a Source Report.


You can leave a comment for a particular entry in the Source tab by:

- clicking the  icon found at the end of that component's row and selecting Comments from the dropdown menu or clicking the  icon if there are already comments present.
- clicking the entry in the Source view, clicking the Name of the component, clicking the  icon, and then selecting Comments from the dropdown menu or by clicking the  icon if there are already comments present.

Policy Management Enhancement - Project Groups

Black Duck users will now have the ability to apply policy rules to project group(s) and its descendants. To do so, go to **Policy Management** and either click the **Create Policy Rule** button or the  button and select **Edit**. When the Create/Edit Policy Rule modal opens, ensure the **A Subset of Projects, filtered by...** option is enabled to see the Project Conditions filter dropdown.

Policy Management Enhancement - Added (RCE) Remote Code Execution to Vulnerability Conditions

Black Duck users will now have the ability to add Remote Code Execution (RCE) as a filter option when creating or editing policies. To do so, go to **Policy Management** and either click the **Create Policy Rule** button or the  button and select **Edit**. The new (RCE) Remote Code Execution value will be displayed in the Vulnerability Conditions dropdown menu.

Changes to Project Group Manager permissions

Previously, the actual permissions of the Project Group Manager were not affected by the global settings

for allowing a project manager to remediate vulnerabilities or override policy. Now, the Project Group Manager role permissions will be adjusted based on Project Manager Role Settings.

Supported browser versions

- Safari Version 15.0 (16612.1.29.41.4, 16612)
 - Safari versions 13.0 and below are no longer supported
- Chrome Version 94.0.4606.71 (Official Build) (x86_64)
- Firefox Version 92.0.1 (64-bit)
- Microsoft Edge Version 94.0.992.38 (Official build) (64-bit)
 - Microsoft Edge versions 79 and below are no longer supported

Container versions

- blackducksoftware/blackduck-postgres:9.6-1.3
- blackducksoftware/blackduck-authentication:2021.10.0
- blackducksoftware/blackduck-webapp:2021.10.0
- blackducksoftware/blackduck-scan:2021.10.0
- blackducksoftware/blackduck-jobrunner:2021.10.0
- blackducksoftware/blackduck-cfssl:1.0.4
- blackducksoftware/blackduck-logstash:1.0.11
- blackducksoftware/blackduck-registration:2021.10.0
- blackducksoftware/blackduck-nginx:2.0.9
- blackducksoftware/blackduck-documentation:2021.10.0
- blackducksoftware/blackduck-upload-cache:1.0.19
- blackducksoftware/blackduck-redis:2021.10.0
- blackducksoftware/blackduck-bomengine:2021.10.0
- blackducksoftware/blackduck-matchengine:2021.10.0
- blackducksoftware/blackduck-webui:2021.10.0
- sigsynopsys/bdba-worker:2021.9.1
- blackducksoftware/rabbitmq:1.2.5

API Enhancements

Permission fixes to GET /api/project-groups

The following fixes have been made to the `GET /api/project-groups` api endpoints:

- `GET /api/project-groups` will only return the project groups the user is authorized to view as search results.
- `GET /api/project-groups/<project group ID>` will return a HTTP 200 OK for users with the Super User role or a HTTP 403 FORBIDDEN response otherwise.

Permission changes to GET /api/users/{userId}

The `GET /api/users/{userId}` endpoint now no longer has a permission check (previously required a

USERMGMT_READ check).

- The GET /api/users/endpoint (that lists all users) will continue to be protected with the USERMGMT_READ permissions.
- The projectOwner user (regardless of the user's permission status) in the /api/projects/{projectId} API will still be provided.
- The USERMGMT_READ permission that was added to project roles in Black Duck version 2021.8.2 will still be removed.

New filter parameter for GET /api/project-groups

A new filter parameter called `exactName` has been added to help find specific project groups. When true, the `exactName` filter will ensure only the project group that matches the name value in `q` is returned. The search criteria for the project group is case-insensitive. If none match, then nothing is returned. Also, the `q` parameter must be specified when the `exactName` filter is true otherwise no project groups will be returned.

See below for how the filter is used in a /api/project-groups request:

```
/api/project-groups?q=name:<project group name>&filter=exactName:true
```

Improved CPE Support APIs

Three new public APIs have been added:

- GET /api/cpes [Requires a searchParam. Returns matching CPE IDs]
- GET /api/cpes/{cpeId}/versions [Returns component-versions matching the CPE ID]
- GET /api/cpes/{cpeId}/variants [Returns component-origins matching the CPE ID]

Copyright 2.0 data and new legacy endpoint

Black Duck is now rolling out Copyright 2.0 data using the existing endpoint (below) to serve this new copyright data. No response fields are being dropped or added.

```
GET /api/components/{componentId}/versions/{componentVersionId}/origin/{originId}/file-copyrights
```

We will continue to serve Copyright 1.0 (aka legacy) data by creating a new endpoint :

```
GET /api/components/{componentId}/versions/{componentVersionId}/origin/{originId}/file-copyrights-legacy
```

Note: This new endpoint is not directly used in Black Duck UI, only through the public API directly. Also, since the existing endpoint will now return Copyright 2.0 data, all Black Duck customers (regardless of the version they use) should see this new data.

Exposure of lastScanDate through a Public API

The following API will now expose `lastScanDate` in the Public API response:

- GET /api/projects/{projectId}/versions/{projectVersionId}/bom-status

Fixed Issues in 2021.10.0

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

- (HUB-29413). Searching for components in the Add Component or Edit Component modals is now more accurate, and Custom Components are more easily found.
- (HUB-26545 and HUB-30185). Fixed an issue where the following Public REST API endpoints did not update the componentModification, componentModified, and componentPurpose component conditions as expected.
 - /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}
 - /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}
- (HUB-30474). Fixed an issue where the count displayed on the Affected Projects page was not matching the actual results when the user has no access to certain projects.
- (HUB-30623). Fixed issues where a number of client-initiated errors were creating heavy log churn via logging of stacktraces or were incorrectly logged at a more severe log level than they actually represented.
- (HUB-30099). Fixed an issue where Vulnerability statuses were not updated for existing BOMs by KB update. BoM Component-Version Vulnerability remediations (found in the BoM-security view) will now be updated by the KB Update Job when the remediation status changes if the current status is not user or system updated.
- (HUB-29773). Fixed an issue where the /api/projects/<project ID>/versions/<version ID>/vulnerable-bom-components endpoint would have longer than expected response times. The request now only includes one license definition per version BOM component which should improve the response time. Users should only see a lower number of results if they had a Protex BOM imported with license overrides.
- (HUB-26924). Fixed an issue so that a user-friendly error message now appears when a SAML SSO user login fails. If the SSO configuration is wrong, an error page will be displayed to indicate a configuration issue. If the user is disabled in HUB, an error page will be displayed, notifying the user to contact the system administrator or Unauthorized page.
- (HUB-31176). Fixed an issue where Rapid Scan policy evaluation was not checking the BOM status when the remediation status is associated with a specific project-version.
- (HUB-30808). Fixed an issue where custom fields created under the BOM Component tab in Custom Fields Management were not returning when reviewing a component's "Additional fields" within any project's BOM. We will display up to 100 custom fields when editing the custom fields on BOM component.
- (HUB-30922). Fixed an issue where the descriptions on the Project Version level were not displayed. This field will now display the description used on the Project level.
- (HUB-31482). Fixed an issue where licenses were not shown on the Snippet confirmation page after HUB 2021.6.2.
- (HUB-31003). Fixed an issue where users could get a HTTP 500 Internal Server Error when attempting to perform bulk remediation for vulnerabilities.
- (HUB-31425). Fixed an issue where the Version Detail Report was taking a significant amount of time to run/complete the query when started compared to previous versions of HUB.

- (HUB-29598). Fixed an issue where the number of vulnerabilities in the PDF generated by "Print" button on component page would get pushed out due to the bar being too long.
- (HUB-30133). Fixed an issue where the t-shirt sizing ymls in the helm deployments have the webui container with less memory for an XL deployment than large. The webui container's memory limit is increased to 1024 Mi in x-large.yaml tshirt size.
- (HUB-28889). Fixed an issue where the BOM Engine could fail to start if RabbitMQ is not reachable.
- (HUB-30215). Fixed an issue where BDSA-2020-1311 was incorrectly reporting a workaround was available.
- (HUB-30857). Fixed a bug where the "Affected Projects" page for vulnerabilities was omitting vulnerabilities from ignored components in the items displayed but including them when finding the count for the total items. Now the count for total items also omits vulnerabilities from ignored components.
- (HUB-30603). Fixed an issue where a user could see the entirety of a comment under a BDSA or CVE record under the security tab of a project if it was grayed out.
- (HUB-28753). Fixed an issue where the BomEngine did not accept the value of the HUB_PROXY_PASSWORD_FILE secret when created in docker and would return a 407 AUTHENTICATION REQUIRED error.
- (HUB-31483). Fixed an issue where the policy override date and user information in the Policy Violations modal was displayed incorrectly the Japanese localization.

Version 2021.8.5

New and Changed Features in Version 2021.8.5

Black Duck version 2021.8.5 is a maintenance release and contains no new or changed features.

Fixed Issues in 2021.8.5

- (HUB-31482). Fixed an issue where licenses were not shown on the Snippet confirmation page after Black Duck version 2021.6.2.
- (HUB-31663). Fixed an issue where the QuartzSearchDashboardRefreshJob could get into a condition where it tries to schedule multiple instances of this job causing a large amount of blocked queries.

Container versions

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.8.5
- blackducksoftware/blackduck-webapp:2021.8.5
- blackducksoftware/blackduck-scan:2021.8.5
- blackducksoftware/blackduck-jobrunner:2021.8.5
- blackducksoftware/blackduck-cfssl:1.0.3
- blackducksoftware/blackduck-logstash:1.0.10
- blackducksoftware/blackduck-registration:2021.8.5
- blackducksoftware/blackduck-nginx:2.0.6

- blackducksoftware/blackduck-documentation:2021.8.5
- blackducksoftware/blackduck-upload-cache:1.0.18
- blackducksoftware/blackduck-redis:2021.8.5
- blackducksoftware/blackduck-bomengine:2021.8.5
- blackducksoftware/blackduck-matchengine:2021.8.5
- blackducksoftware/blackduck-webui:2021.8.5
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

Version 2021.8.4

New and Changed Features in Version 2021.8.4

Black Duck version 2021.8.4 is a maintenance release and contains no new or changed features.

Fixed Issues in 2021.8.4

- (HUB-31425). Fixed an issue where the Version Detail Report was taking a significant amount of time to run/complete the query when started compared to previous versions of HUB.

Container versions

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.8.4
- blackducksoftware/blackduck-webapp:2021.8.4
- blackducksoftware/blackduck-scan:2021.8.4
- blackducksoftware/blackduck-jobrunner:2021.8.4
- blackducksoftware/blackduck-cfssl:1.0.3
- blackducksoftware/blackduck-logstash:1.0.10
- blackducksoftware/blackduck-registration:2021.8.4
- blackducksoftware/blackduck-nginx:2.0.6
- blackducksoftware/blackduck-documentation:2021.8.4
- blackducksoftware/blackduck-upload-cache:1.0.18
- blackducksoftware/blackduck-redis:2021.8.4
- blackducksoftware/blackduck-bomengine:2021.8.4
- blackducksoftware/blackduck-matchengine:2021.8.4
- blackducksoftware/blackduck-webui:2021.8.4

- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

Version 2021.8.3

New and Changed Features in Version 2021.8.3

Reporting database enhancements

Added the following data to scan_stats_view under the reporting schema:

- scan_size

Fixed Issues in 2021.8.3

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

- (HUB-29959, HUB-30391, and HUB-30397). Fixed an issue where scans would not complete due to a 500 Internal Error response from the KnowledgeBase while preparing the Bill of Materials.
- (HUB-31047). Fixed an issue when populating the version BOM components page, the UI makes duplicate calls to the back-end generating unnecessary stress to the database.
- (HUB-30074). Fixed an issue where very small code locations snippet scans sometimes finish before upload source info is updated giving the appearance that the uploaded source was lost.

Container versions

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.8.3
- blackducksoftware/blackduck-webapp:2021.8.3
- blackducksoftware/blackduck-scan:2021.8.3
- blackducksoftware/blackduck-jobrunner:2021.8.3
- blackducksoftware/blackduck-cfssl:1.0.3
- blackducksoftware/blackduck-logstash:1.0.10
- blackducksoftware/blackduck-registration:2021.8.3
- blackducksoftware/blackduck-nginx:2.0.6
- blackducksoftware/blackduck-documentation:2021.8.3
- blackducksoftware/blackduck-upload-cache:1.0.18
- blackducksoftware/blackduck-redis:2021.8.3
- blackducksoftware/blackduck-bomengine:2021.8.3
- blackducksoftware/blackduck-matchengine:2021.8.3
- blackducksoftware/blackduck-webui:2021.8.3
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

Version 2021.8.2

New and Changed Features in Version 2021.8.2

Black Duck version 2021.8.2 is a maintenance release and contains no new or changed features.

Fixed Issues in 2021.8.2

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

- (HUB-31078). Documented an issue where install and upgrade to Black Duck 2021.8 would fail in Kubernetes when the `--reuse-values` flag is used as part of the installation/upgrade. Please refer to the REAME.md under Helm charts for more details.
- (HUB-31086). Fixed an issue where the snippets box at top right side of BOM Page was missing for few project versions.
- (HUB-31156). Fixed an issue where users with the Project level BOM Manager role and without any Global or Overall roles would not able to access the Project BOM.

Container versions

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.8.2
- blackducksoftware/blackduck-webapp:2021.8.2
- blackducksoftware/blackduck-scan:2021.8.2
- blackducksoftware/blackduck-jobrunner:2021.8.2
- blackducksoftware/blackduck-cfssl:1.0.3
- blackducksoftware/blackduck-logstash:1.0.10
- blackducksoftware/blackduck-registration:2021.8.2
- blackducksoftware/blackduck-nginx:2.0.6
- blackducksoftware/blackduck-documentation:2021.8.2
- blackducksoftware/blackduck-upload-cache:1.0.18
- blackducksoftware/blackduck-redis:2021.8.2
- blackducksoftware/blackduck-bomengine:2021.8.2
- blackducksoftware/blackduck-matchengine:2021.8.2
- blackducksoftware/blackduck-webui:2021.8.2
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

Version 2021.8.1

New and Changed Features in Version 2021.8.1

Black Duck version 2021.8.1 is a maintenance release and contains no new or changed features.

Fixed Issues in 2021.8.1

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

- (HUB-31029). Fixed an issue where the Project Manager Role settings was overriding the individual/group's Super User role.
- (HUB-30808). Fixed an issue where custom fields created under the BOM Component tab in Custom Fields Management were not returning when reviewing a component's "Additional fields" within any project's BOM.
- (HUB-30655). Fixed an issue where users without the Super User role could see "Project Group Management" option in the Management menu.
- (HUB-31077). Fixed an issue where upgrading Black Duck HUB from 2021.6.0 to 2021.8.x would fail for Kubernetes deployments due to a change made to a property in the helm chart. Other prior versions are unaffected.

Container versions

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.8.1
- blackducksoftware/blackduck-webapp:2021.8.1
- blackducksoftware/blackduck-scan:2021.8.1
- blackducksoftware/blackduck-jobrunner:2021.8.1
- blackducksoftware/blackduck-cfssl:1.0.3
- blackducksoftware/blackduck-logstash:1.0.10
- blackducksoftware/blackduck-registration:2021.8.1
- blackducksoftware/blackduck-nginx:2.0.6
- blackducksoftware/blackduck-documentation:2021.8.1
- blackducksoftware/blackduck-upload-cache:1.0.18
- blackducksoftware/blackduck-redis:2021.8.1
- blackducksoftware/blackduck-bomengine:2021.8.1
- blackducksoftware/blackduck-matchengine:2021.8.1
- blackducksoftware/blackduck-webui:2021.8.1
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

Version 2021.8.0

New and Changed Features in Version 2021.8.0

PostgreSQL 13 support for external databases

Black Duck now supports and recommends PostgreSQL 13 for new installs that use external PostgreSQL. Migrating to 2021.8.x does not require migration to PostgreSQL 13.

No action is required for users of the internal PostgreSQL container.

Please note that PostgreSQL 12 is not supported.

Installation documentation will be updated in an upcoming release.

Notice for Azure customers

Support for Black Duck on Azure PostgreSQL 13 will be best-effort only with no guarantee of resolution until Azure PostgreSQL 13 is fully released. As such, we very strongly recommend against using Azure PostgreSQL 13 for production deployments and customer should use Azure PostgreSQL 11.

For more information on Azure support for PostgreSQL 13, please visit <https://docs.microsoft.com/en-us/azure/postgresql/concepts-version-policy>.

New System Setting for scans: Component Dependency Duplication Sensitivity

This setting allows users to change how the system displays duplicate package ID's for components on the Source page that are found during scans. In previous releases and as the default setting in 2021.8.0 (set to 1), the Source page will only display one package ID discovery regardless of how often it is found in your scan. Changing this setting to greater than 1 will display more entries allowing for greater layer-by-layer insight to help determine from which layer each component originated. This feature is especially useful to customers who are scanning in Detect with BOM aggregation enabled and want to see package ID references across the various modules that have been aggregated into 1 scan.

New System Setting for scans: Minimum Scan Interval

This setting allows users to change the minimum hourly frequency of which signature scans can be performed for a given code location when using the LCA enhanced signature scanning. The default setting is set to 0, or no minimum scan interval, meaning scans are not prevented from occurring regardless of frequency. If set to greater than 0, signature scans will not be processed if they occur before the set scan interval. For example, a setting of 4 will not allow signature rescans before 4 hours of time have elapsed. This setting may be configured globally in the Administration > System Settings > Scan page or through the Detect client as a command line option. Note: This setting is only used if customer scan using the parameter `--detect.blackduck.signature.scanner.arguments='--signature-generation'`.

Note: When this feature is enabled, signature scans with Detect will finish with a status of success even if the signature scan was not run due to the scan interval. A warning message will appear in the logs indicating the scan was not run, but there will be no other indication given to the user.

Changes in Rapid Scan policy application

Rapid Scan users now have the ability to configure how policies are applied to the results of Full (traditional) scans, Rapid Scans, or both. The default setting for new installations of Black Duck starting from version 2021.8.0 will be set to apply to full scans only. To use Rapid Scan to fetch all vulnerabilities regardless of policies, simply create a single policy, setting the condition severity `>=0`.

Added phone-home cumulative count of the number of rapid scans done

This count is accurate and data is not lost, but there might be some timing issues where some of the scans are from the subsequent day's data.

Rapid Scan vulnerability conditions added to Policy Management

The following vulnerability conditions are now available in Policy Management:

- CWE IDs
- Solution Available
- Workaround Available
- Exploit Available
- Reachable from Source
- Remediation Status

Project Group Management

Black Duck now provides the ability to logically group all your projects in the Hub, allowing you to organize which projects belong to which business unit making it easier for you to view risk across the organization. Project groups can contain both projects and other project groups to provide a multi-level hierarchy.

Users and Groups can be assigned to Project Groups with any number of roles. That assignment will give those users access to the projects below that group with the specified roles unless that assignment is explicitly overridden at the lower levels. This concept allows for setting users with default access to projects that haven't been created yet.

In addition, the search dashboard has been enhanced to return search results for projects the user has access to via a project group.

New Global Release Creator, Project Group BOM Annotator user roles, and changes to existing roles

The Project Creator and Global Code Scanner roles have had their access to the Global Release Create permission revoked and will no longer be able to create releases of projects they do not own or have access to. A new role, Global Release Creator, has been made to fill in the gap for users who depended on this functionality. All current users with Project Creator and/or Global Code Scanner will automatically inherit this role as part of the upgrade migration script. That means this change will be specifically opt-out for current users looking to take advantage of the more narrow security change.

The Project Group BOM Annotator has the BOM Annotator permissions for every project in the assigned project group. This means they can add or edit comments and edit custom fields for projects associated with the project group.

Protex BOM Tool token access support enhancement

The Protex BOM tool now supports the `BD_HUB_TOKEN` environment variable to upload json exported from Protex to the Hub. You can set the token by adding "-T " using command prompt.

Add `BD_HUB_TOKEN=[insert token here]` variable to `.bash_profile` to make the change permanent.

Vulnerability Notifications enhancement

Added a new environment variable: `BLACKDUCK_NOTIFY_WHEN_REMEDIATED` in the `blackduck-config.ev` file. It defaults to true, but when set to false Black Duck will no longer send/create "new" vulnerability notifications for vulnerabilities with a remediation status of "Ignored, Remediation Complete, Mitigated, or Patched."

Signature scan timeout message enhancement

Network timeouts during a signature scan (waiting for a response from HUB) now return an accurate error message that indicates a network timeout and not an I/O error (code 74). The new message format will display `Scan <Corresponding Scan ID> failed: [<Reason why it happened and whether to contact an administrator or retry the scan>]`.

Request Retry mechanism for Black Duck Hub enhancement

A waiter has been introduced which will retry uploading the scan to Hub when it receives HTTP 502/503/504 responses. It will retry in increments of 30 seconds for 10 minutes before declaring that the scan is failed.

Scans page enhancement

A new Created column was added to the Scans page allowing you to see when the scan was created. The date displayed in the column will make it easier to compare dates when filtering scans using the Created Date option.

Surface license risk info for Components without versions

New logic has been introduced to determine a default license for components with an unknown version. This is an estimated license based on greatest number of times it shows up across the top 1,000 versions of the component. With this, you will be able to calculate license risk without requiring a version to be selected. It is, however, recommended that you review these components and manually specify a version for more accurate results.

Reporting database enhancements

Added the following data to `scan_stats_view` under the reporting schema:

- `user_id`
- `project_id`
- `project_name`
- `version_id`
- `version_name`
- `scan_id`
- `scan_name`
- `code_location_id`
- `code_location_name`
- `scan_type`
- `scan_status`
- `scan_start_at`
- `scan_end_at`
- `scan_duration`
- `scan_age`

- scan_archived_at
- application_id

Policy rule condition enhancement

A new policy condition operator was added for policy rules Vulnerability Conditions Category for Overall Score. You may now select "Less than or equal to" when creating or editing policy rules.

API enhancements

- New API added that enables bulk confirm/un-confirm ignore/un-ignore of snippet matches.
 - PUT /api/projects/{projectId}/versions/{versionId}/bulk-snippet-bom-entries Media Type: application/vnd.blackducksoftware.bill-of-materials-6+json
- The following API endpoints have been updated to consider projects the user can access via project group membership. The query parameter has also changed from name to entityName for parity with the response content.
 - GET /api/users/{userId}/assignable-projects
 - GET /api/users/{userId}/assignable-project-groups/
 - GET /api/usergroups/{userGroupId}/assignable-projects
 - GET /api/usergroups/{userGroupId}/assignable-project-groups

Container versions

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.8.0
- blackducksoftware/blackduck-webapp:2021.8.0
- blackducksoftware/blackduck-scan:2021.8.0
- blackducksoftware/blackduck-jobrunner:2021.8.0
- blackducksoftware/blackduck-cfssl:1.0.3
- blackducksoftware/blackduck-logstash:1.0.10
- blackducksoftware/blackduck-registration:2021.8.0
- blackducksoftware/blackduck-nginx:2.0.5
- blackducksoftware/blackduck-documentation:2021.8.0
- blackducksoftware/blackduck-upload-cache:1.0.18
- blackducksoftware/blackduck-redis:2021.8.0
- blackducksoftware/blackduck-bomengine:2021.8.0
- blackducksoftware/blackduck-matchengine:2021.8.0
- blackducksoftware/blackduck-webui:2021.8.0
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

Fixed Issues in 2021.8.0

- (HUB-29341). Fixed an issue when exporting BOM from Protex using the `--include-files` flag and then importing it to a Hub instance would generate a Java heap space error.
- (HUB-29005). Fixed an issue where if a BOM has two components with the exact same name but different UUIDs, the filter API `(/api/projects/projectId/versions/versionId/components-filters?filterKey=bomComponents)` should return two separate components based on ID and their versions (if present) rather than grouping them by name.
- (HUB-29567). Fixed an issue where the “Updated” (or “Last Settings Update” in 2021.8.0) timestamp would be updated but not the updated by user name on the Project version > Details view. The “Last Settings Update” timestamp and updated by user name will now only be updated when project version details are changed.
- (HUB-30139). Fixed an issue in the Protex BOM tool where an Unmarshalling Error: Illegal character occurred when using the `--include-files` flag.
- (HUB-12280). Fixed an issue where uploading a bdio file with relationships to the project are not visible when they are also located lower in the 'bdio tree'.
- (HUB-29481). Fixed an issue where licenses with the same name but different capital letters were being omitted from notices reports.
- (HUB-30143). Fixed an issue where the Protex BOM tool 2021.6.0 did not work with latest JDK (11.0.11).
- (HUB-29274). Fixed an issue where VersionReportJob could cause jobrunner Out Of Memory issue when there are circular references on BOM page.
- (HUB-29381). Fixed an issue when a project version is added as a component (using Add > Project), the component entry would show an invalid Operational Risk level.
- (HUB-30087). Fixed an issue where the project version query fails to find the version when version name includes multi-byte alpha-numeric characters.
- (HUB-23686). Fixed an issue when running Detect against a node file the signature scanner would get stuck.
- (HUB-25592). Fixed an issue where component (or component version)'s adjustments got dropped automatically from BOM.
- (HUB-25552). Fixed an issue where component (or component version) with 'MATCH' type adjustments were automatically added/deleted from BOM.
- (HUB-29196). Fixed an issue where the policy violation pop-up did not disappear when it was clicked and the mouse cursor was moved away from the policy violation symbol quickly.
- (HUB-29573). Fixed an issue where line breaks in a policy rule's description were ignored when viewing the policy violation modal.
- (HUB-30611). Fixed an issue with where numeric usernames were causing errors in a database migration script.
- (HUB-26611). Fixed an issue where Direct/Transitive dependencies were not reported correctly when using aggregation in Detect. Please note that this fix is resolved only when using Detect 7.4 and requires using the new SUBPROJECT `detect.bom.aggregate.remediation.mode` in Detect.
- (HUB-22379). Fixed performance issues where project tagging and having tag policy can take hours on some instances.

- (HUB-30141). Fixed an issue with Hub swarm docker-compose.yml containing the unsupported "links" options.
- (HUB-29549). Fixed a performance issue with the loading of the BOM page caused by permission checks.

Version 2021.6.2

New and Changed Features in Version 2021.6.2

Black Duck version 2021.6.2 is a maintenance release and contains no new or changed features.

Container versions

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.6.2
- blackducksoftware/blackduck-webapp:2021.6.2
- blackducksoftware/blackduck-scan:2021.6.2
- blackducksoftware/blackduck-jobrunner:2021.6.2
- blackducksoftware/blackduck-cfssl:1.0.2
- blackducksoftware/blackduck-logstash:1.0.10
- blackducksoftware/blackduck-registration:2021.6.2
- blackducksoftware/blackduck-nginx:2.0.5
- blackducksoftware/blackduck-documentation:2021.6.2
- blackducksoftware/blackduck-upload-cache:1.0.17
- blackducksoftware/blackduck-redis:2021.6.2
- blackducksoftware/blackduck-bomengine:2021.6.2
- blackducksoftware/blackduck-matchengine:2021.6.2
- blackducksoftware/blackduck-webui:2021.6.2
- sigsynopsys/bdba-worker:2021.06
- blackducksoftware/rabbitmq:1.2.2

Fixed Issues in 2021.6.2

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

- (HUB-30493). Fixed an issue where the Blackduck Alert instance was not accessible for hosted users due to specifying the proxy certificate location for Alert in NGINX configuration.

Version 2021.6.1

New and Changed Features in Version 2021.6.1

Black Duck Security Advisory (BDSA) Remote Code Execution Exposure

Black Duck highlights vulnerabilities that may allow Remote Code Execution (RCE) in the 2021.6.1 release. In the Black Duck UI, if the BDSA vulnerability has a RCE tag it will appear in the full BDSA record, the table

of vulnerabilities, and in the Security tab of a particular component.

The vulnerability APIs report the vulnerability using an array with the name `bdsaTags`. If the `bdsaTag` array includes “RCE” then that vulnerability may allow Remote Code Execution.

- `/api/components/{componentId}/vulnerabilities`
- `/api/components/{componentId}/versions/{componentVersionId}/vulnerabilities`
- `/api/components/{componentId}/versions/{componentVersionId}/origin/{componentVersionOriginId}/vulnerabilities`
- `/api/projects/{projectId}/versions/{versionId}/components/{componentId}/versions/{componentVersionId}/origins/{componentVersionOriginId}/vulnerabilities`

Container versions

- `blackducksoftware/blackduck-postgres:9.6-1.1`
- `blackducksoftware/blackduck-datadog:1.0.1`
- `blackducksoftware/blackduck-solr:1.0.0`
- `blackducksoftware/blackduck-authentication:2021.6.1`
- `blackducksoftware/blackduck-webapp:2021.6.1`
- `blackducksoftware/blackduck-scan:2021.6.1`
- `blackducksoftware/blackduck-jobrunner:2021.6.1`
- `blackducksoftware/blackduck-cfssl:1.0.2`
- `blackducksoftware/blackduck-logstash:1.0.10`
- `blackducksoftware/blackduck-registration:2021.6.1`
- `blackducksoftware/blackduck-nginx:2.0.3`
- `blackducksoftware/blackduck-documentation:2021.6.1`
- `blackducksoftware/blackduck-upload-cache:1.0.17`
- `blackducksoftware/blackduck-redis:2021.6.1`
- `blackducksoftware/blackduck-bomengine:2021.6.1`
- `blackducksoftware/blackduck-matchengine:2021.6.1`
- `blackducksoftware/blackduck-webui:2021.6.1`
- `sigsynopsys/bdba-worker:2021.06`
- `blackducksoftware/rabbitmq:1.2.2`

Fixed Issues in 2021.6.1

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

- (HUB-29202). Fixed an issue where the binary scan container(`bdba-worker`) of 2021.4.0 did not work on docker SWARM by increasing timeout and retry values.
- (HUB-29405). Fixed an issue where matches were being dropped, due to the identification of a `core_i7` architecture.

- (HUB-30134). Fixed an issue where the BOM engine silently fails to start due to RabbitMQ connectivity issue.
- (HUB-30170). Fixed an issue where Redis fails to start due to incorrect configuration in the docker-entrypoint when utilizing dual stack Kubernetes.
- (HUB-30202). Fixed an issue where the vulnerability details page does not correctly change the display of the score metrics when the user clicks from BDSA scoring to NVD scoring and vice versa.

Version 2021.6.0

New and Changed Features in Version 2021.6.0

New containers and changes to system requirements

In the 2021.6.0 release:

- A new container, blackduck-webui, has been added for improved Black Duck performance, better caching, and future scalability.
- The Rapid Scanning feature is now available to all Black Duck customers. This feature requires a new container, blackduck-matchengine, which manages connections to the Black Duck KnowledgeBase and cache KnowledgeBase results for short intervals.

The following are now the minimum hardware that will be needed to run a single instance of all containers. Note that memory requirements depend on the number of concurrent Rapid Scans you want to support.

- 7 CPUs
- 28.5 GB RAM for the minimum Redis configuration; 31.5 GB RAM for an optimal configuration providing higher availability for Redis-driven caching. This will support up to 100 concurrent Rapid Scans.

30 GB RAM for the minimum Redis configuration; 33 GB RAM for an optimal configuration providing higher availability for Redis-driven caching. This will support more than 150 Rapid Scans, however, the maximum number of supported Rapid Scans is still being determined.
- 250 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

The following is the minimum hardware that is needed to run Black Duck with Black Duck - Binary Analysis.

- 8 CPUs
- 32.5 GB RAM for the minimum Redis configuration; 35.5 GB RAM for an optimal configuration providing higher availability for Redis-driven caching. This will support up to 100 concurrent Rapid Scans.

34 GB RAM for the minimum Redis configuration; 37 GB RAM for an optimal configuration providing higher availability for Redis-driven caching. This will support more than 150 Rapid Scans, however, the maximum number of supported Rapid Scans is still being determined.
- 350 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

Note: An additional CPU, 2 GB RAM, and 100 GB of free disk space will be needed for every additional binaryscanner container.

Rapid Scanning

Rapid Scanning is now available for all customers.

Black Duck's Rapid Scanning provides a way for developers to quickly determine if the versions of open source components included in a project violate corporate policies surrounding the use of open source. Using Synopsys Detect, Rapid Scanning quickly returns results as it only employs package manager scanning and does not interact with the Black Duck server database. Use Rapid Scanning when you need quick feedback and when persisting the data in Black Duck is not necessary.

Using Rapid Scanning enables you to run thousands of scans while eliminating the need to deploy additional instances of Black Duck. It provides you with actionable results (such as failing the build) that can be used without a project version or without access to Black Duck's user interface.

New jobs subsystem

The jobs subsystem has been replaced with a new implementation.

- Possible status for a job can now be:
 - Pending
 - In progress
 - Complete
 - Error
- You can filter jobs based on their schedule: periodic or on demand.
- With the new implementation, the following jobs have been added:
 - BomAggregatePurgeOrphansCheckJob. Checks to see if any BOM data is not associated with a project version and starts the necessary jobs.
 - BomVulnerabilityDataRecomputationCheckJob. Checks if BOM computations are required when certain settings change and starts the necessary jobs.
 - BomVulnerabilityDataRecomputationJob. Updates component information received from the KnowledgeBase.
 - HierarchicalVersionBomCheckJob. Checks if hierarchical BOM computations are required and starts the necessary jobs to process them
 - JobHistoryStatsJob-Calculate Daily Statistics. Calculates daily statistics based on job activity.
 - JobHistoryStatsJob-Calculate Five Minute Statistics. Calculates statistics in 5-minute intervals based on job activity.
 - JobHistoryStatsJob-Calculate Hourly Statistics. Calculates statistics in one-hour periods based on job activity.
 - JobHistoryStatsJob-Prune Job History. Prunes old records from the job history based on the retention settings.
 - KBUpdateCheckJob. Initiates updates received from the KnowledgeBase.
 - KbUpdateWorkflowJob-BDSA Vulnerability Update. Updates BDSA vulnerability information

received from the KnowledgeBase.

- KbUpdateWorkflowJob-Component Update. Updates component information received from the KnowledgeBase.
- KbUpdateWorkflowJob-Component Version Update. Processes component version updates received from the KnowledgeBase.
- KbUpdateWorkflowJob-License Update. Updates license information received from the KnowledgeBase.
- KbUpdateWorkflowJob-NVD Vulnerability Update. Updates NVD vulnerability information received from the KnowledgeBase.
- KbUpdateWorkflowJob-Summary.Issues a summary report about the most recent KnowledgeBase update.
- LicenseTermFulfillmentCheckJob. Checks if license fulfillment processing is required and starts the necessary jobs.
- NotificationPurgeCheckJob. Checks if there are notifications that need cleanup and starts the necessary jobs.
- QuartzVersionBomEventCleanupJob. Cleans up BOM events based on the retention policy.
- VersionBomComputationCheckJob. Checks if BOM computations are required and starts the necessary jobs to process them.
- VersionBomNotificationCheckJob. Issues notifications for BOM computation results.
- WatchdogJob. Monitors recurring jobs to ensure they are running properly and reports on or fixes issues as they are determined.

- The following jobs have been removed:

- KbUpdateJob

Report enhancements

- A new project version report, `license_conflicts_date_time.csv` has been added. It lists the license conflicts for this project version. This report has the following columns:
 - Component id
 - Version id
 - Component name
 - Component version name
 - Usage
 - License ids
 - License names
 - Source/Type
 - License Term Responsibility
 - License Term Category
 - License Term Name
 - Description
 - Conflicting License Id

- Conflicting License Name
 - Conflicting License Term Source Type
 - Conflicting License Term Responsibility
 - Conflicting License Term Category
 - Conflicting License Term Name
 - Conflicting License Term Description
- A new column, Has License Conflicts, has been added to the end of the `components_date_time.csv` project version report. This column indicates whether this component version has a license conflict.
 - File names for reports now use the system timezone instead of UTC.

Ability to refresh Black Duck KnowledgeBase copyright information

Black Duck now provides the ability for you to view updated Black Duck KnowledgeBase copyright information for a component origin. If there is new or updated data, Black Duck updates the information shown while keeping any edits that you made.

New role

A new role, BOM Annotator, has been added to Black Duck. Users with this role have read-only access to a project and can add or edit comments in a BOM and update BOM custom fields.

LDAP or SAML group synchronization

if you enabled group synchronization when configuring LDAP or SAML for Black Duck, the name of this group in the external authentication system (LDAP or SSO) now appears in the **External Group Name** field on the *Group Name* page. Now, if a group names changes on the external system, you can edit it to keep the Black Duck group name in sync with the external authentication system group name.

Enforcement of required custom fields

Black Duck now provides an option so that users *must* enter values when editing objects which have required custom fields.

New filters for project search

Black Duck now provides these filters when searching for projects:

- Never Scanned. Use this filter to find all project versions that were never part of a scan.
- Not Scanned Since. Use this filter to find all project version that have not been scanned since the selected time period.

Retention period for unmapped code locations

The default retention period for unmapped code locations has changed from 365 days to 30 days.

Additional information in the Add/Edit Component dialog boxes

So that you can more easily determine the component you wish to use, the Add Component and Edit Component dialog boxes now include the component's home page URL and the number of project versions that use this component.

Policy enhancements

The following component conditions now include a "false" option:

- License Conflict with Project Version
- Unfulfilled License Terms
- Unknown Component Version

Improved C/C++ matching

In the 2021.6.0 release, BOM accuracy has been improved for customers scanning C/C++ in the Linux domain.

New match types

Two new match types have been added in the 2021.6.0 release.

- Direct Dependency Binary. Scanning identified that the binaries in use are a direct dependency.
- Transitive Dependency Binary. Scanning identified that the binaries in use are a transitive dependency.

API enhancements

- With the change to the jobs subsystem:
 - The `GET /jobs/{jobID}` This call gets the job details for a specific job by ID. This call will now return a 404 Not Found status code.
 - The following calls are out-of-service since Black Duck version 2020.2.0, returning a 404 Not Found status code, and will remain non-functional in Black Duck version 2021.6.0:
 - `PUT /jobs/{jobID}` This call reschedules a job.
 - `DELETE /jobs/{jobID}` This call terminates a job.

The functionality will be replaced with a new Job Rest API implementation which will be available in a future release.

- Added new boolean field to policy view (`/api/policy-rules/{policyRuleId}`) expressions ("developerScanExpression") to identify rapid scan types.

Supported browser versions

- Safari Version 14.0.3 (15610.4.3.1.7, 15610)
- Chrome Version 90.0.4430.72 (Official Build) (x86_64)
- Firefox Version 88.0 (64-bit)
- Microsoft Edge Version 90.0.818.41 (Official build) (64-bit)

Container versions

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.6.0
- blackducksoftware/blackduck-webapp:2021.6.0
- blackducksoftware/blackduck-scan:2021.6.0

- blackducksoftware/blackduck-jobrunner:2021.6.0
- blackducksoftware/blackduck-cfssl:1.0.2
- blackducksoftware/blackduck-logstash:1.0.10
- blackducksoftware/blackduck-registration:2021.6.0
- blackducksoftware/blackduck-nginx:2.0.0
- blackducksoftware/blackduck-documentation:2021.6.0
- blackducksoftware/blackduck-upload-cache:1.0.17
- blackducksoftware/blackduck-redis:2021.6.0
- blackducksoftware/blackduck-bomengine:2021.6.0
- blackducksoftware/blackduck-matchengine:2021.6.0
- blackducksoftware/blackduck-webui:2021.6.0
- sigsynopsys/bdba-worker:2021.03
- blackducksoftware/rabbitmq:1.2.2

Japanese language

The 2021.4.0 version of the UI, online help, and release notes has been localized to Japanese.

Fixed Issues in 2021.6.0

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

- (Hub-21613). Fixed an issue where the scan.cli version 2019.8.x displayed a non-meaningful warning message about performance degradation due to Java version used.
- (Hub-25227, 25521). Fixed an issue where the scan's status of Scan Complete on the Scans page was misleading.
- (Hub-26108). Fixed an issue where deploying Black Duck with Alert when using a customer certificate required manual intervention with the nginx alert configuration file.
- (Hub-26924). Fixed an issue so that a user-friendly error message now appears when a SAML SSO user login fails.
- (Hub-27209). Fixed an issue where the VersionBomComputationJob failed with the following error: "Error in job execution: could not extract ResultSet; SQL [n/a]; constraint [cvss2_severity]."
- (Hub-27681). Fixed an issue whereby the BOM Engine had to be started by a root user when deployed on Kubernetes with a custom security context.
- (Hub-27894). Fixed an issue so that the reset is set to 0 in new Black Duck searches.
- (Hub-28171). Fixed an issue where the copyright search failed for one project.
- (Hub-28305). Fixed an issue where the following error was seen in the logs: Failed class com.blackducksoftware.job.integration.domain.impl.JobMaintenanceJob.
- (Hub-28347). Fixed an issue whereby a snippet adjustment resulted in a duplicate key SnippetAdjustment error.
- (Hub-28351). Fixed a performance issue when saving BOM license changes.
- (Hub-28469). Fixed an issue where custom certificates could not be configured with Docker 20.10.x.
- (Hub-28726). Fixed an issue whereby Black Duck displayed the name of the user who cloned a

project as the name of the component reviewer after the project was cloned.

- (Hub-28909). Fixed an issue where an incorrect error message appeared in the Black Duck UI after a user account was locked out.
- (Hub-29071). Fixed an issue with performance when bulk editing snippets.
- (Hub-29168). Fixed an issue where if there were no matches in a scan that was mapped to a project version, then project-level file adjustments were not applied to that project version.

Version 2021.4.1

New and Changed Features in Version 2021.4.1

Black Duck version 2021.4.1 is a maintenance release and contains no new or changed features.

Fixed Issues in 2021.4.1

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

- (Hub-28347). Fixed an issue where bulk snippet adjustments failed with the following error: "Adjustment Failed: The server encountered an error, please check your connection and try again."
- (Hub-28807). Fixed an issue where the following error was seen in the Artifactory plugin: "Too many parameters error on /api/projects/<projectID>/versions/<projectVersionID>/components/<componentID>/versions/<componentVersionID>?offset=0&limit=100."
- (Hub-29002). Fixed an issue where filtering for unignored snippets in the Snippet Confirmation window displayed system-wide snippets.
- (Hub-29448). Fixed an issue where the LDAP user authorization failed with an IncorrectResultSizeDataAccessException error.

Version 2021.4.0

New and Changed Features in Version 2021.4.0

Rapid Scanning - Limited Customer Availability feature

Black Duck's Rapid Scanning provides a way for developers to quickly determine if the versions of open source components included in a project violate corporate policies surrounding the use of open source. Using Synopsys Detect, Rapid Scanning quickly returns results as it only employs package manager scanning and does not interact with the Black Duck server database. Use Rapid Scanning when you need quick feedback and when persisting the data in Black Duck is not necessary.

Using Rapid Scanning enables you to run thousands of scans while eliminating the need to deploy additional instances of Black Duck. It provides you with actionable results (such as failing the build) that can be used without a project version or without access to Black Duck's user interface.

Note: Rapid Scanning is a limited customer access feature in the 2021.4.0 release. To use Rapid Scanning, contact your Synopsys account management team for assistance.

Duplicate BOM detection

Black Duck has added duplicate BOM detection which determines if a new package manager scan

duplicates the existing BOM, and if so, stops processing the scan and denotes it as complete. For high-frequency scans that generate redundant (identical) data, Black Duck's duplicate BOM detection can provide significant performance improvements.

In Black Duck 2021.4.0, this feature only impacts package manager (dependency) scans when the set of dependencies discovered by Synopsys Detect is identical to the set from the previous scan. This capability will be extended in future releases.

Ability to configure Project Manager role

Black Duck now provides the ability for system administrators to define whether the Project Manager role can manage policy violations (override policy violations or remove overrides) or remediate security vulnerabilities for a project.

By default, users with the Project Manager role can manage policy violations and remediate security vulnerabilities: users upgrading to version 2021.4.0 will not see any changes in the Project Manager role.

Multi-license editing enhancements

When editing a license for a KnowledgeBase or custom component version, Black Duck now gives you the ability to easily create new or edit existing multi-license scenarios for the components at the root level or at the same level as the original license.

Deep license data enhancement

Black Duck now provides the ability to add file level deep licenses or remove a manually added license.

Report enhancements

- The following enhancements were made to the component project version report (`component_date_time.csv`):
 - A new column, Component origin id, has been added to the end of the report. This column provides the component origin ID value that previously could only be obtained using the API.
 - The user name, date, and time was added to each comment listed in the Comments column.
- A new column, Knowledgebase Timed Out, has been added to the end of the upgrade guidance project version report (`project_version_upgrade_guidance_date_time.csv`). It indicates whether or not a Black Duck KnowledgeBase timeout error occurred while fetching upgrade guidance data for a component version/origin.

Policy management enhancements

- Project and component conditions available for a policy rule have been reorganized into categories to make it easier to find and select a condition. Also, custom fields for projects and components have been separated by the type of custom field.
- A new license condition, License Expiration Date Comparison for declared or deep licenses, lets you compare a license expiration date with the release date for a project version.

Vulnerability Impact enhancement

A new vulnerability condition for policy rules, Reachable from Source, is now available enabling you to create policy rules for vulnerabilities which have been identified as reachable. Use this condition to prioritize those vulnerabilities with a different (higher) priority.

Changes to LDAP or SAML group synchronization

To reduce authentication errors, Black Duck has modified LDAP or SAML group synchronization. Now, if you enabled group synchronization when configuring LDAP or SAML for Black Duck, group names on your LDAP or SAML server and the Black Duck server must be identical. If you change the name of a group in Black Duck, you must also change the name of the group on your LDAP or SAML server to match the new name (and vice versa). If the names are not identical, then the groups may be out-of-sync and user permissions for that group will be lost.

Container enhancement

A health check was added to the Binaryscanner container.

Enhancement to the Source tab

A new filter, Code View Available, has been added to the project version **Source** tab.

Component and project search enhancement

The Find page for component and project searches now provides the ability to sort search results.

Saved search enhancement

Sorted search results are supported for saved searches letting you view the results in the interested order on the Dashboard page.

Performance improvement to the *Project Name* page

To improve performance, you now must select the policy violation icon (⚠) or override icon (⚙) to view policy violation information on the **Overview** tab on the *Project Name* page.

Cloning enhancements

The following enhancements were made to cloning a project version:

- The default cloning options have changed. Now, all cloning options are enabled when a project is created.
- A new option, **Version Settings**, has been added which clones these values:
 - License
 - Notes
 - Nickname
 - Release Date
 - Phase
 - Distribution
- A new Clone Version dialog box appears when you select **Clone** from the *Project Name* page. If the **Version Settings** cloning option is enabled, only the new version name appears in the dialog box.
- To eliminate confusion, the **Version to Clone** field has been removed from the Create a New Version dialog box.

License conflicts enhancement

Manual edits to a BOM, including changing the usage for a component or the license of the project version

using the **License Conflicts** or **Components** tab will now trigger a recalculation of the license conflict.

Enhancements to the System Information page

The usage categories on the System Information page have been enhanced.

- In the **usage: project** section, the "Scans by project" section now lists "Top 10 scans by project."
- In the **usage: rapid scan completion** section, "Rapid Scans by User" now lists the "Top 10 rapid scans by User."
- The **usage: scan completion** section has been reformatted into tables and includes an "identical package manager" row for duplicate BOM detection. Two new tables have also been added: "Code location summary information" and "Duplicate BOM information."

These pages show six months of data or the number of months the system has data, whichever value is smaller.

A new job, CollectScanStatsJob, collects scan statistics shown on the **usage: scan completion** section on the System Information page.

Removal of installation guides

The *Installing Black Duck using Kubernetes* and the *Installing Black Duck using OpenShift* guides have been removed from the documentation set. These documents only contained links to the latest documentation. These links have been added to the Black Duck documentation page in each PDF and to the home page of the online help.

Enhancement to the Project Name page

The *Project Name* page has been reorganized and enhanced and now includes the last scanned date for each project version.

Enhancement to the Dashboard page

The Policy Violations value for "None" in the Policy Violations Pie Chart on the Dashboard page previously returned either 100% (no violations) or 0% (some violations), now reflects the actual percentage for violations.

API enhancements

- Added the capability to generate Postman collections in the API documentation through `/api-doc/postman-collection-public.json`. Users can import the `postman-collection-public.json` file as a Postman collection into Postman.
- Added the capability to generate OpenAPI Specification (OAS) for customer-facing endpoints through `/api-doc/openapi3-public.json`.
- Added the capability to filter projects by project owner by using `/api/projects?filter=owner`, which takes the URL of the user to search for the user-owned projects, for example, `/api/projects?filter=owner:https://<bd_server>/api/users/`.
- Added license ownership information as a new ownership field to the `/projects/`

`{projectId}/versions/{projectVersionId}/components` endpoint.

■ Added APIs for reading and altering the following application settings:

- Reading analysis settings

`GET /api/settings/analysis`

- Updating analysis settings

`PUT /api/settings/analysis`

- Reading branding settings

`GET /api/settings/branding`

- Updating branding settings

`PUT /api/settings/branding`

- Reading license review settings

`GET /api/settings/license-review`

- Updating license review settings

`PUT /api/settings/license-review`

- Reading role settings

`GET /api/settings/role`

- Updating role settings

`PUT /api/settings/role`

- Added `/api/component-migrations` and `/api/component-migrations/{componentOrVersionId}` endpoints to get component migration data based on specific dates or specific components from the KnowledgeBase.
- Made the `/license-dashboard` API public, which allows a user to see the in-use licenses.
- Resolved an issue with the `api/vulnerabilities/{vulnerabilityId}` endpoint returning a header overflow error when the vulnerability had over 100 references. The endpoint now provides a warning and includes meta links in the response body when 25 or more link headers are returned in the response headers.
- Removed the "Trigger type" filter from the Activity/Journal endpoints as it is only used for the "user" type.

Supported browser versions

- Safari Version 14.0.3 (15610.4.3.1.7, 15610)
- Chrome Version 90.0.4430.72 (Official Build) (x86_64)

- Firefox Version 88.0 (64-bit)
- Microsoft Edge Version 90.0.818.41 (Official build) (64-bit)

Container versions

- blackducksoftware/blackduck-postgres:1.0.16
- blackducksoftware/blackduck-authentication:2021.4.0
- blackducksoftware/blackduck-webapp:2021.4.0
- blackducksoftware/blackduck-scan:2021.4.0
- blackducksoftware/blackduck-jobrunner:2021.4.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.9
- blackducksoftware/blackduck-registration:2021.4.0
- blackducksoftware/blackduck-nginx:1.0.31
- blackducksoftware/blackduck-documentation:2021.4.0
- blackducksoftware/blackduck-upload-cache:1.0.16
- blackducksoftware/blackduck-redis:2021.4.0
- blackducksoftware/blackduck-bomengine:2021.4.0
- sigsynopsys/bdba-worker:2021.03
- blackducksoftware/rabbitmq:1.2.2

Japanese language

The 2021.2.0 version of the UI, online help, and release notes has been localized to Japanese.

Fixed Issues in 2021.4.0

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

- (Hub-24015, 26281). Fixed an intermittent permission denied error seen in the Black Duck user interface.
- (HUB-25116). Fixed an issue where red dots appeared in the Snippet View dialog box for a file encoded in UCS-2, rendering the text unreadable.
- (HUB-25549). Fixed an issue with `/api/uploads` where the created code location was not mapped to the project version when `codeLocationName` contained Japanese characters.
- (HUB-25550). Added BOM update information to a project version's activity/journal.
- (HUB-25605, 27618). Fixed an issue when using `/api/tokens/authenticate` to authenticate with an API token, where after the token expired, the HTTP client got redirected to the SAML provider page or an error occurred when generating PDF reports.
- (Hub-25993). Fixed an issue where a duplicate record caused the following error message to appear in the job runner log: 'A conflicting object already exists.'
- (Hub-26481). Fixed an issue where a page would refresh completely after saving a new remediation status.
- (HUB-26588). Fixed an issue where running a binary scan on android-studio-ide-201.7199119-

windows.exe failed.

- (Hub-26695). Fixed an issue where scans took significantly longer during certain times of the day.
- (Hub-26897). Fixed an issue so that a 404 Not Found error code appears for invalid versions which are those not listed on the *Component Name* page.
- (Hub-26911). Fixed an issue where selecting an alternate snippet match incorrectly identified a component as having cryptography.
- (Hub-27159). Fixed an issue for policy rules using the 'Contributors in the past year', 'Commits in the past year' or 'New Version Count' component conditions. Although these conditions were defined to trigger a violation if the value was equal to 0, policy violations were triggered when the value was greater than 0 or a component had no commit history.

Note: With this fix, new scans or rescans may remove some policy violations that were previously triggered.

- (Hub-27167). Fixed an issue whereby active users assigned to an inactive group with the Global Project Viewer role could see all projects in the Dashboard.
- (Hub-27175). Fixed an issue where the **Used count** value on the *Component Name* page was inaccurate as it was based on the number of component origins, not the component versions.
- (Hub-27282). Fixed an issue where the policy violation popup in the BOM occasionally got stuck open and could not be closed unless the page was refreshed.
- (Hub-27284, 27660). Fixed an issue where some dynamically linked components with a match type of transitive dependency were missing the match information in the **Source** column in the project version BOM.
- (Hub-27287). Fixed an issue so that risk counts shown on the **Overview** tab on the *Project Name* page use component version values (as the BOM page does), instead of by component origin.
- (Hub-27293). Fixed an issue where components marked as Reviewed were noted as Unreviewed when the project was rescanned.
- (Hub-27306). Fixed an issue where components were listed in case sensitive order in the Notices Report.
- (Hub-27308). Fixed an issue where the Black Duck KB *Component Name* page did not correctly show the number of vulnerabilities after the license for a component version was changed.
- (Hub-27326). Fixed an issue whereby deleting the application ID using the project's **Settings** tab did not actually delete the application ID.
- (Hub-27613). Fixed an issue where the source files for binaries could not be navigated in the **Source** tab.
- (Hub-27961). Fixed the legends for the graphs on the Dashboard page so that they did not appear clickable.
- (Hub-27982). Fixed an issue where the binary scan only identified the first and last files in an MSI archive.
- (Hub-27985). Fixed an issue with the message that appears when Black Duck is building the BOM which would disappear when you scrolled down the BOM page.
- (Hub-28094). Fixed an issue where the `/api/usergroups` endpoint was not properly using "_" or "%" in the search term.

- (Hub-28165). Fixed an issue with editing a license on the BOM page where selecting Cancel/Close still applied the changes.
- (Hub-28208). Fixed an issue where the code base size shown on the Registration page was incorrect.
- (Hub-28226). Fixed an issue so that components that are in violation of one or more policies will now generate a "policy cleared" notification when the code location that brought them in is unmapped or deleted.
- (Hub-28259). Fixed an issue with an unreview/unignore SQL query analysis.
- (Hub-28292). Fixed an issue where the HELM t-shirt sizing `.yaml` files did not scale the BOM engine container.
- (Hub-28370). Fixed an issue where critical vulnerabilities were not shown when using the comparison view of the BOM.
- (Hub-28375). Fixed an issue so that the **Affected Projects** tab for a CVE or BDDB record no longer displays vulnerabilities from components that have been ignored.
- (Hub-28383). Fixed an issue where if the *Project Name* page was filtered and as a result only one version appeared on the page, the version could not be deleted.
- (Hub-28416). Fixed an issue where the AND or OR operator for a group of licenses could not be modified.
- (Hub-28458). Fixed an issue where the SnippetScanAutoBom job displayed an "Error in job execution: Duplicate key" error message.
- (Hub-28562). Fixed an issue with a binary scan where the scan failed to complete post work and the following error message appeared: "Path is not a parent of null."
- (Hub-28580). Fixed an issue when attempting to access the **My Access Tokens** page caused the following error "The application has encountered an unknown error."
- (Hub-28639). Fixed an issue where the suffix of the downloaded report file had a `.json` extension instead of `.zip` if the project name contained both English and Chinese characters.
- (Hub-28681). Fixed an issue so that the usage is shown on the **Source** tab when the match type is direct or transitive dependency.
- (Hub-28765). Fixed an issue where the BOM page displayed snippets that were both confirmed and ignored.
- (Hub-28773). Fixed an issue so that TLSv1.1 was removed from the TLS_PROTOCOLS option in the `hub-webserver.env` file.

Version 2021.2.1

New and Changed Features in Version 2021.2.1

Black Duck version 2021.2.1 is a maintenance release and contains no new or changed features.

Fixed Issues in 2021.2.1

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

- (Hub-23928). Fixed an issue where a confirmed snippet match was changed after a rescan.
- (Hub-26898). Fixed an issue whereby a scan appeared to be completed, however, Synopsys Detect timed out as it failed to get a bom_complete notification from Black Duck.

- (Hub-27688). Fixed an issue whereby the API call for matched files returned no information for transitive and direct dependency matches.
- (Hub-28410). Fixed an issue where the RabbitMQ container could not be started on Kubernetes which was resolved by introducing a persistent volume.
- (Hub-28208, 28386). Fixed an issue whereby the incorrect code base size was displayed on the Product Registration page.
- (Hub-28278). Fixed an issue where a missing persistent volume for RabbitMQ container caused excessive logging in the BOM Engine and scan failures.
- (Hub-28292). Fixed an issue with scaling the BOM Engine container.

Version 2021.2.0

New and Changed Features in Version 2021.2.0

New custom vulnerability dashboards

So that you can easily view the vulnerabilities that are important to you, in 2021.2.0, the Security Dashboard has been replaced with custom vulnerability dashboards based on your saved vulnerability searches. Black Duck now provides the ability for you to search for vulnerabilities used in your projects and/or the Black Duck KnowledgeBase using a variety of attributes, save the search, and then use the Dashboard page to view dashboards from those saved searches.

For each vulnerability, the custom vulnerability dashboard displays the following information:

- BDSA or NVD vulnerability ID. Selecting the vulnerability ID shows more information on the vulnerability, such as additional score values.
- Number of project versions affected by this vulnerability with a link to view the **Affected Projects** tab for the vulnerability which lists the project versions affected by this vulnerability.
- Overall risk score.
- Whether a solution, workaround, or exploit is available.
- Date when a vulnerability was first detected, published, and last modified.
- Common Weakness Enumeration (CWE) number for this security vulnerability.

Vulnerability search enhancements

Searching for vulnerabilities has been enhanced by the attributes you can use to search for the vulnerability and the information shown in the search results. You can select whether to search for vulnerabilities in your projects or vulnerabilities in the Black Duck KnowledgeBase.

The following attributes are available when searching for vulnerabilities:

- Affecting projects
- Default Remediation
- Reachable
- Exploit
- First Detected
- Remediation Status

- Solution
- Base Score
- Exploitability Score
- Impact Score
- Overall Score
- Published Year
- Severity
- Source (BDSA or NVD)
- Temporal Score
- Workaround

These vulnerability search results can now be saved and view in the Dashboard page, as described previously.

Ability to manage license conflicts for projects

To reduce the risk of license infringement, you need to understand when a component in your BOM has a license with terms that are incompatible with the declared license of a project. Black Duck now identifies these license term conflicts and displays them on a new **License Conflict** tab located on the **Legal** tab.

You can also set a policy rule that is triggered when a component's license is in conflict with the license of a project version.

Note that Black Duck only determines license conflicts for component versions with high license risk. For the Black Duck license risk model, "high risk" means that licenses in this family tend to have license conflicts under this business scenario (combination of distribution type and component usage) making them incompatible. Medium or low risks means it may have risks if the business scenario changes (or is defined incorrectly) or due to other, non-license conflicts factors.

Dependencies

When direct or transitive dependencies are found in a Synopsys Detect scan, Black Duck now lists the number of matches for each type of dependency in the project version's **Security** tab.

For transitive dependencies, a dependency tree shows the components that brought in this dependency, the vulnerabilities by severity level, and a match count for the number of times the component was brought in with that dependency path.

Report database enhancements

A new table for ignored components, (`component_ignored`), has been added to the report database. It has these columns:

- `id`. ID
- `project_version_id`. Project version ID.
- `component_id`. Component ID.
- `component_version_id`. Component version ID.
- `component_name`. Component name.

- `component_version_name`. Component version name.
- `version_origin_id`. Version origin ID.
- `origin_id`. Origin ID.
- `origin_name`. Origin name.
- `ignored`. Boolean that indicates whether the component is ignored.
- `policy_approval_status`. Policy approval status.
- `review_status`. Review status of the component.
- `reviewed_by`. User who reviewed the component.
- `reviewed_on`. When the component was reviewed.
- `security_critical_count`. Number of critical security vulnerabilities.
- `security_high_count`. Number of high security vulnerabilities.
- `security_medium_count`. Number of medium security vulnerabilities.
- `security_low_count`. Number of low security vulnerabilities.
- `security_ok_count`. Number of no security vulnerabilities.
- `license_high_count`. Number of high license risk.
- `license_medium_count`. Number of medium license risk.
- `license_low_count`. Number of low license risk.
- `license_ok_count`. Number of no license risk.
- `operational_high_count`. Number of high operational risk.
- `operational_medium_count`. Number of medium operational risk.
- `operational_low_count`. Number of low operational risk.
- `operational_ok_count`. Number of ok operational risk.

A new table for user information, `user`, has been added to the report database. It has these columns.

- `id`. ID.
- `first_name`. User's first name.
- `last_name`. User's last name.
- `username`. User's username in Black Duck.
- `email`. User's email address.
- `active`. A boolean that indicates whether this user is active.
- `last_login`. Time that the user last logged in to Black Duck.

License editing enhancements

The following enhancements were made when editing licenses in the BOM.

- When editing a license for a component, Black Duck now gives you the ability to easily create new or edit existing multi-license scenarios for the components in your BOM at the root level or at the same level as the original license.
- If you selected a different license for a component, you can now revert the license to its original license as defined in the Black Duck KnowledgeBase.

- A new option in the *Component Name Version* Component License dialog box makes it easily discernible that there is an edit mode.

Report enhancement

A new column, Archive Context and Path, has been added to the end of the `source_date_time.csv` project version report. This column concatenates the information shown in the existing Path and Archive Content columns to provide the full path for each component.

Notices File Report

The Notices File Report has been improved so that copyright data no longer contains duplicate information for a single component-origin.

Binary scan enhancement

Binary scans now return partial matches in addition to full matches.

Deep license data enhancement

When reviewing evidence of deep license data in a file, Black Duck now highlights the license text that triggered the license text match.

BOM Engine

To improve Black Duck UI response time, license updates will now be performed by the BOM Engine. This process can be seen as a "License Update" or "License Term Fulfillment Update" event in the BOM Processing Status dialog box, accessible from the BOM.

Black Duck tutorials

To easily view training for Black Duck, you can now select **Black Duck Tutorials** from the Help menu (



) in the Black Duck UI.

Modification to password configuration

Users with the System Administrator role can now set password requirements for local Black Duck accounts. Users with the Super User role can no longer configure password requirements.

Policy rule enhancement

Policy management now provides the ability to create policy rules based on project version custom fields for Boolean, Date, Drop Down, Multiple Selections, Single Selection, and Text field types.

Hosting location for Synopsys Detect

Black Duck customers with limited external connectivity can now define the internal hosting location of Synopsys Detect. Using this information, these users can leverage Code Sight for deployment across their developer base to run on-demand Software Composition Analysis (SCA) scans.

Saved search dashboard enhancements

For each saved search shown on the Dashboard page, Black Duck now lists the date and time the search was last updated. A popup displays the saved search filters with a link so that you can open the Find page

to edit and save a revised saved search.

Snippet triage enhancement

Icons have been added to the **Source** tab to make it easier to differentiate unconfirmed (⚠), confirmed (☑), and ignored (⊖) snippets.

Supported browser versions

- Safari Version 14.0.3 (15610.4.3.1.6, 15610)
- Chrome Version 88.0.4324.150 (Official Build) (x86_64)
- Firefox Version 85.0.2 (64-bit)
- Microsoft Edge Version 88.0.705.63 (Official build) (64-bit)

Container versions

- blackducksoftware/blackduck-postgres:1.0.16
- blackducksoftware/blackduck-authentication:2021.2.0
- blackducksoftware/blackduck-webapp:2021.2.0
- blackducksoftware/blackduck-scan:2021.2.0
- blackducksoftware/blackduck-jobrunner:2021.2.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.9
- blackducksoftware/blackduck-registration:2021.2.0
- blackducksoftware/blackduck-nginx:1.0.30
- blackducksoftware/blackduck-documentation:2021.2.0
- blackducksoftware/blackduck-upload-cache:1.0.15
- blackducksoftware/blackduck-redis:2021.2.0
- blackducksoftware/blackduck-bomengine:2021.2.0
- sigsynopsys/bdba-worker:2020.12-1
- blackducksoftware/rabbitmq:1.2.2

Supported Docker versions

Black Duck installation supports Docker versions 18.09.x, 19.03.x, and 20.10.x (CE or EE).

Docker webapp-volume

The Docker webapp-volume is no longer used in orchestration. Optionally, users can backup and prune the Docker webapp-volume; otherwise no action is required.

API enhancements

- API documentation is now only available at <https://<Black Duck server URL>/api-doc/public.html>.
- Added the capability to filter code locations (/api/codelocations) by creation date.
- Fixed the API used to download the SAML Identity Provider Metadata XML file (api/sso/idp-metadata endpoint) that was working incorrectly in previous versions.

- The remediation-guidance endpoint (GET /api/components/{componentId}/versions/{componentVersionId}/remediating) no longer returns a “410 GONE” response. You must switch to the upgrade-guidance endpoint, (GET /api/components/{componentId}/versions/{componentVersionId}/upgrade-guidance) which is incompatible with the remediation-guidance endpoint that was removed.
- Added a report dependency-paths endpoint to show dependency paths for a component:
`/api/project/{projectId}/version/{projectVersionId}/origin/{originId}/dependency-paths`
- Added the Synopsys Detect URI endpoint which is only used to set or update reading the Synopsys Detect URI on the System Settings page:
`/external-config/detect-uri`

Ubuntu operating system

The preferred operating system for installing Black Duck in a Docker environment for Ubuntu is now version 18.04.x.

Japanese language

The 2020.12.0 version of the UI, online help, and release notes has been localized to Japanese.

Fixed Issues in 2021.2.0

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

- (Hub-22103). Fixed an issue whereby the Black Duck server did not respond in time when updating a license status.
- (Hub-22623). Fixed an issue whereby the Summary Dashboard frequently timed out for enterprise customers when loading in the UI.
- (Hub-24332). Fixed an issue where scanning the same code location caused duplicated notifications.
- (Hub-25374). Fixed a permission error for database azure_maintenance.
- (Hub-25580). Fixed an issue whereby components shown in the BOM were incorrectly sorted after page 9.
- (Hub-25666). Fixed a pagination issue for the endpoint /usergroups/<group #>/roles.
- (Hub-26030). Fixed an issue where sorting options were not retained for a dashboard by project name after performing an action.
- (Hub-26324). Fixed an issue where the following error "java.lang.IllegalStateException: Parent of [file:/C:/src/External/PackageManager/ProjectTemplates/com.unity.template.universal-10.1.0.tgz] does not exist" occurred when uploading a scan.
- (Hub-26343). Fixed an issue where Black Duck could not be registered as the registration container ran out of heap space.
- (Hub-26493). Fixed a confusing error message which appeared when a user removed themselves as a member of a project.
- (Hub-26501). Fixed an issue whereby the cordova-plugin-inappbrowser component could not be selected in the Edit Component dialog box.
- (Hub-26536). Fixed an issue whereby a watched project displayed the Unwatched icon (👁) in the

page header.

- (Hub-26540). Fixed an issue whereby the initial configuration of SAML did not go into effect unless Black Duck was restarted.
- (Hub-26615). Fixed an issue whereby a user with the Project Manager role in Project A and Project Manager and Project Code Scanner roles in Project B could upload scans to Project A.
- (Hub-26616). Fixed an issue whereby attempting to ignore a snippet would fail with the following error message: "Unable to update existing snippet adjustment because changing the consumer, producer, adjustment type, start line, end line is not supported."
- (Hub-26712, 26962). Fixed an issue whereby the snippet icon shown in the tree view on the **Source** tab did not clear after a snippet match was confirmed.
- (Hub-26726). Fixed an issue whereby the "not in" option was not available for custom fields when creating a policy rule.
- (Hub-26807). Fixed an issue whereby a HTML status code 404 was received when attempting to GET custom fields for the BOM component version.
- (Hub-26815). Fixed an issue whereby saving SAML integration settings caused the page to reload and switch Identity Provider Metadata settings.
- (Hub-26904). Fixed an issue whereby the match count value shown on the project version **Activity** section on the **Settings** tab was not the same as on the *Scan Name* page.
- (Hub-26930). Fixed an issue where notifications were not triggered for a component.
- (Hub-27002). Fixed an issue whereby the wrong notification was sent when a cloned project was created.
- (Hub-27049). Fixed an issue whereby the License Terms category for a Project Version Report could not be seen in the Black Duck UI without a user being assigned the License Manager role.
- (Hub-27208). Fixed an issue with blackduck-nginx whereby Synopsys Alert failed to load when SAML was configured.
- (Hub-27227). Fixed an issue whereby snippet matching took a long time to complete.
- (Hub-27264). Fixed an issue whereby reviewing a component reset its usage to its default value.
- (Hub-27681). Fixed an issue whereby the BOM Engine had to be started by a root user when deployed on Kubernetes with a custom security context.

Version 2020.12.0

New and Changed Features in Version 2020.12.0

New containers and changes to system requirements

There are two additional containers: BOM Engine and RabbitMQ (now a required container) for the 2020.12.0 release.

The minimum system requirements to run a single instance of all containers are:

- 6 CPUs
- 26 GB RAM for the minimum Redis configuration; 29 GB RAM for an optimal configuration providing higher availability for Redis-driven caching

- 250 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

The minimum hardware that is needed to run Black Duck with Black Duck - Binary Analysis are:

- 7 CPUs
- 30 GB RAM for the minimum Redis configuration; 33 GB RAM for an optimal configuration providing higher availability for Redis-driven caching
- 350 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

Note: An additional CPU, 2 GB RAM, and 100 GB of free disk space will be needed for every additional binaryscanner container.

Password configuration

Users with the Super User role can now set password requirements for *local* Black Duck accounts. If enabled, Black Duck ensures that the new password meets your requirements and also rejects passwords that are considered weak, such as "password", "blackduck", or a user's username or email address.

Super Users can:

- define the minimum password length.
- define the minimum number of character types for the password. Possible character types are lowercase letters, uppercase letters, numbers, or special characters.
- select whether to enforce the password requirements on current users when they log in to Black Duck.

By default, *password requirements are enabled* and have these settings:

- The minimum password length is eight characters.
- Only one character type is required.
- Password requirements are not enforced on current users when logging in to Black Duck.

License enhancements

So that you can successfully manage license risk, Black Duck now gives you the ability to create new or edit existing multi-license scenarios for the components in your BOM.

Vulnerability Impact Analysis enhancements

- A new project version report, `vulnerability_matches_date_time.csv`, has been added. It lists the component, vulnerability data, and vulnerability impact analysis data for each component potentially reached by a vulnerability. This report has the following columns:
 - Component name
 - Component id
 - In use
 - Component version name
 - Version id

- Channel version origin
 - Origin id
 - Origin name id
 - Vulnerability Id
 - Vulnerability source
 - CVSS Version
 - Security Risk
 - Base score
 - Overall score
 - Solution available
 - Workaround available
 - Exploit available
 - Called Function
 - Qualified Name
 - Line Number
- A new table, vulnerability method matches (`vulnerability_method_matches`), has been added to the report database. It has the following columns:
 - `id`. ID.
 - `project_version_id`. UUID of the project version where the reachable vulnerability appears.
 - `vuln_source`. Source of the vulnerability. For vulnerability impact analysis, the value is BDSA.
 - `vuln_id`. Vulnerability ID, such as BDSA-2020-1234.
 - `qualified_name`. Name of the class the function is called on.
 - `called_function`. Name of the vulnerable function call in your code that makes the vulnerability reachable.
 - `line_number`. Line number in your code where the vulnerable function is called.
 - The vulnerability reports (vulnerability remediation report, vulnerability status report, and the vulnerability update report) now have a new column, "Reachable", added to the end of the report, to denote whether the security vulnerability is reachable (true) or not reachable (false).

BOM computation information

Black Duck now provides detailed information on the status of the computation of the project version BOM.

The new **Status** indicator (replacing the Components indicator) in the project version header in the Black Duck UI provides the current status of the BOM and notifies you of the state of the processing of BOM events. For more information, a new BOM Processing Status dialog box lists the events that are pending, processing, or have failed.

Black Duck also provides the ability to configure the frequency of the BOM event cleanup job (`VersionBomEventCleanupJob`) which clears those BOM events that might be stuck because of processing errors or topology changes.

Policy enhancements

- Policy management now provides the ability to create policy rules based on these custom fields:
 - Component custom fields for Boolean, Date, Drop Down, Multiple Selections, Single Selection, and Text field types.
 - Component version custom fields for Boolean, Date, Drop Down, Multiple Selections, Single Selection, and Text field types.
- You can now distinguish between declared and deep (embedded) license data when creating policy rules for these conditions:
 - License
 - License expiration date
 - License family

Note: Any existing policy rules using these license conditions will now only apply to declared licenses. You must create a separate policy rule for deep (embedded) licenses for these license conditions.

Report enhancements

The vulnerability reports (vulnerability remediation report, vulnerability status report, and the vulnerability update report) that were previously only available at the global or project level are now available for project versions.

Configuration of snippet file size

You can now modify the default maximum file size that will be scanned for snippets and select a value from 1MB to 16MB.

Configuration of the clean up of unmapped code locations

Black Duck purges unmapped code location data every 365 days. You can disable this feature, such that unmapped code location data is not purged, or set the retention period to a lower number of days if you scan regularly and want to discard the data frequently.

Access tokens

The options for the scope of user access tokens are now Read or Read and Write.

Supported browser versions

- Safari Version 14.0.1 (14610.2.11.51.10)
- Chrome Version 87.0.4280.88 (Official Build) (x86_64)
- Firefox 83.0 (64-bit)
- Internet Explorer 11 11.630.19041.0

Note that support for Internet Explorer 11 is deprecated and Synopsys will be ending support for Internet Explorer 11 starting with the Black Duck 2021.2.0 release.

- Microsoft Edge 87.0.664.60 (Official build) (64-bit)

Container versions

- blackducksoftware/blackduck-postgres:1.0.16
- blackducksoftware/blackduck-authentication:2020.12.0
- blackducksoftware/blackduck-webapp:2020.12.0
- blackducksoftware/blackduck-scan:2020.12.0
- blackducksoftware/blackduck-jobrunner:2020.12.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.8
- blackducksoftware/blackduck-registration:2020.12.0
- blackducksoftware/blackduck-nginx:1.0.26
- blackducksoftware/blackduck-documentation:2020.12.0
- blackducksoftware/blackduck-upload-cache:1.0.15
- blackducksoftware/blackduck-redis:2020.12.0
- blackducksoftware/blackduck-bomengine:2020.12.0
- sigsynopsys/bdba-worker:2020.09-1
- blackducksoftware/rabbitmq:1.2.2

API enhancements

- Added ability to sort projects (api/projects) by the createdAt field.
- Added the ability to filter to the api/projects endpoint for projects created before/after a date.
- Added the API for displaying vulnerability matches as part of the Vulnerability Impact Analysis feature.

GET /api/projects/{projectId}/versions/{projectVersionId}/vulnerabilities/{vulnerabilityId}/vulnerability-matches

- Added the following BOM endpoints:

- Get BOM status summary:

GET /api/projects/{projectId}/versions/{projectVersionId}/bom-status

- List a BOM's events:

GET /api/projects/{projectId}/versions/{projectVersionId}/bom-events

- Delete a failed BOM event:

DELETE /api/projects/{projectId}/versions/{projectVersionId}/bom-events/{bomEventId}

- Delete all failed events from a BOM:

DELETE /api/projects/{projectId}/versions/{projectVersionId}/bom-events

- New password settings endpoints:

- Get password settings:

GET /api/password/security/settings

- Get system password settings:

GET /api/password/management/settings

- Update system password settings:

PUT /api/password/management/settings

- Validate password:

POST /api/password/security/validate

- The /api/catalog-risk-profile-dashboard API now returns HTTP 404 (Not Found).

Japanese language

The 2020.10.0 version of the UI, online help, and release notes has been localized to Japanese.

Fixed Issues in 2020.12.0

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

- (Hub-24839). Fixed an issue where some component origin IDs could not be selected from the Add/Edit Component dialog box.
- (Hub-24911). Fixed an issue where a failed KBUUpdateJob skipped component updates.
- (Hub-25230). Fixed an issue where the license text window did not appear when the user attempted to open or edit license text.
- (Hub-25452). Fixed an issue so that the **Discovery Type** filter is automatically added when a license type is selected when viewing license search results page in the **Source** tab.
- (Hub-25489). Fixed an issue where the filter in the **Source** tab was reset when the subfolder was changed.
- (Hub-25603). Fixed an issue so that the path shown in the **Matched File Path** field in the Snippet View dialog box on the **Source** tab refreshed when an alternative path was selected.
- (Hub-25681). Fixed an issue where the Protex BOM Tool failed to import licenses for generic/unspecified component versions.
- (Hub-25715). Fixed an issue where the Active status in the Custom Fields Management page could not be modified unless the mouse was used.
- (Hub-25739). Fixed an issue where all comments for a BOM component could not be viewed.
- (Hub-25874). Fixed an issue where the `bom_component_custom_fields_date_time.csv` report listed different data than the `components_date_time.csv` report even though the data was in the same column name.
- (Hub-26442). Fixed an issue whereby a scan could not be deleted inside a project version by a project owner.
- (Hub-26496). Fixed an issue where a policy violation for license risk was still triggered although the license risk had changed when the component's usage was changed.

Version 2020.10.1

New and Changed Features in Version 2020.10.1

Container versions

- blackducksoftware/blackduck-postgres:1.0.13
- blackducksoftware/blackduck-authentication:2020.10.1
- blackducksoftware/blackduck-webapp:2020.10.1
- blackducksoftware/blackduck-scan:2020.10.1
- blackducksoftware/blackduck-jobrunner:2020.10.1
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.8
- blackducksoftware/blackduck-registration:2020.10.1
- blackducksoftware/blackduck-nginx:1.0.26
- blackducksoftware/blackduck-documentation:2020.10.1
- blackducksoftware/blackduck-upload-cache:1.0.15
- blackducksoftware/blackduck-redis:2020.10.1
- sigsynopsys/bdba-worker:2020.09-1
- blackducksoftware/rabbitmq:1.2.2

Fixed Issues in 2020.10.1

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

- (Hub-25489). Fixed an issue where the filters selected in the **Source** tab were reset when a different folder was selected.
- (Hub-25515). Fixed an issue when the host instance was running TLS 1.3 where the Signature Scanner failed when uploading and displayed the following error message: "ERROR: Unable to secure the connection to the host".
- (Hub-25791). Fixed an issue where significant increases in scan time occurred after upgrading from version 2020.4.2 to version 2020.6.1/2020.6.2.
- (Hub-26027). Fixed an issue where Black Duck displayed the following error message: "ERROR: The application has encountered an unknown error. (Bad Request) error.{core.rest.common_error}" when attempting to upload a Synopsys Detect scan.
- (Hub-26085). Fixed an issue where binary scans added a second empty scan.

Version 2020.10.0

New and Changed Features in Version 2020.10.0

New custom component dashboards

So that you can easily view the component versions that are important to you, in 2020.10.0, the Component Dashboard has been replaced with custom component dashboards based on your saved component

searches. Black Duck now provides the ability for you to search for components used in your projects using a variety of attributes, save the search, and then use the Dashboard page to view dashboards from those saved searches.

For each component version, the custom component dashboards display the following information:

- Number of project versions using this component version and for each project version, the phase, license, review status, and security risks
- Number of vulnerabilities by risk category
- License and operational risk
- Policy violations
- Approval status
- Date the component version was first detected
- Date when the component was released, according to the Black Duck KnowledgeBase
- Number of new versions
- Date when a vulnerability for the component was last updated

Component and Black Duck KnowledgeBase search enhancements

Searching for components has been enhanced by the attributes you can use to search for the component and the information shown in the search results. The UI has also been enhanced so that you can easily differentiate searches for components used in your projects and searches for components in the Black Duck KnowledgeBase.

While the search attributes for Black Duck KnowledgeBase searches has not changed, the following attributes are available when searching for component versions used in your Black Duck projects:

- Security risk
- License risk
- Operational risk
- Policy rule
- Policy violation severity
- Review status
- Component approval status
- First detected
- License family
- Missing custom field data
- Release date
- License
- Vulnerability CWE
- Vulnerability reported date

For each component version matching your search criteria, the following information is shown:

- Number of project versions using this component version and for each project version, the phase, license, review status and security risks
- Number of vulnerabilities by risk category
- License and operational risk
- Policy violations
- Approval status
- Date the component version was first detected
- Date when the component was released, according to the Black Duck KnowledgeBase
- Number of new versions
- Date when a vulnerability for the component was last updated

These component search results can now be saved and view in the Dashboard page, as described previously.

For each KnowledgeBase component search result, the following information is shown:

- Number of project versions that use this component and a list of each project version, its phase, component version used, and associated security risk
- Commit activity trend
- Last commit date
- Number of component versions
- Tags for this component

Enhancement to saved searches

Black Duck now provides the ability to filter and sort saved searches on the Dashboard page.

License conflicts

In the 2020.10.0 release, Black Duck now provides the ability for you to designate incompatible custom license terms. You can define the custom license terms for forbidden or required actions that are in conflict with Black Duck KnowledgeBase terms or with your custom license terms.

Note: Currently, you cannot view incompatible license terms in a project version BOM. This ability will be available in a future Black Duck release.

License Management Enhancements

These three new filters have been added to the **License Terms** tab in License Management:

- Is Associated with License(s)
- Has Incompatible Term(s)
- Responsibility

New component usage

Black Duck has added an "Unspecified" usage which you can use to indicate that you need to investigate the usage of the component. You may find it useful to use this usage as the default value instead of existing

defaults such as Dynamically Linked to eliminate confusion about whether the component is assigned its true usage value or the default value.

New tier

Black Duck has added a tier 0, which you can use to designate as the most critical tier.

Due to this new tier, these default policy rules have been modified to include tier 0:

- No External Tier 0, Tier 1 or Tier 2 Projects With More Than 1 High Vulnerability
- No External Tier 0, Tier 1 or Tier 2 Projects With More Than 3 Medium Vulnerabilities

There is no change to the existing tiers.

Enhancements to custom fields

The following enhancements have been made to custom fields

- Black Duck now provides the ability for you to denote that a custom field is required.
 - A warning message "*" Additional fields are required" appears when viewing custom field information. However, users can still view and save non-custom field information and information for non-required custom fields on the page if data is not entered for the required custom field.
 - A new filter, "Missing Custom Field Data", has been added to the BOM so that you can view those components in the project version BOM which are missing information.
- An option to clear the selection has been added when viewing custom field information for Boolean and single select field types.

Allowed signature lists

Signature lists define the signatures Black Duck sends to the Black Duck KnowledgeBase web service to identify the open source software contained in the your scanned code. The Signature Scanner now has two new parameters which you can use to create allowed signature lists for binary or source file extensions. Each list is optional and works independently of the other list.

- **--BinaryAllowedList *x, y, z*** where *x, y, z* are the approved file extensions for SHA-1 (binary) files.
- **--SourceAllowedList *a, b, c*** where *a, b, c*, are the approved file extensions for clean SHA-1 (source code) files.

Enhancements to vulnerability impact analysis

The following enhancements have been made to vulnerability impact analysis:

- A new column, "Reachable", has been added to the end of the `security_date_time.csv` project version report to denote whether the security vulnerability is reachable (true) or not reachable (false).
- A new filter, "Reachable", has been added to the project version **Security** tab.

Report enhancements

The following reports have been enhanced:

- A new column, "Comments", has been added to the end of the `components_date_time.csv` project version report and lists the comments for each component.

- A new column, "Match type", has been added to the end of the `vulnerability-status-report_date_time.csv` report to identify the match type.

Enhancements to the Report Database

The following columns have been added to the component matches table (`component_matches`):

- `match_confidence`. Represents the confidence in the match, excluding snippet, binary, or partial file matches.
- `match_archive_context`. Local path to the archived file relative to the project's root directory.
- `snippet_confirmation_status`. Review status of the snippet matches.

HTTP/2 and TLS 1.3

To improve security and rendering of the Black Duck UI in a browser, Black Duck now supports HTTP/2 and TLS 1.3 in the Black Duck NGINX webserver. Note that the Black Duck NGINX Webserver continues to support HTTP/1.1 and TLS 1.2.

Change to jobs for purging scans

The `BomVulnerabilityNotificationJob` and the `LicenseTermFulfillmentJob` now also remove old audit events.

API enhancements

- Added an endpoint to determine the Single Sign-On (SSO) status of Black Duck.

GET `/api/sso/status`

- Added endpoints for retrieving SAML/LDAP configurations (Admin use only).

- Read SSO configuration:

GET `/api/sso/configuration`

- Download an IDP metadata file:

GET `/api/sso/idp-metadata`

- These SSO endpoints were also added:

- Update SSO configuration:

POST `/api/sso/configuration`

- Upload an IDP metadata file:

POST `/api/sso/idp-metadata`

- Added the following BOM hierarchical component endpoints:

- List hierarchical root components:

GET `/api/projects/{projectId}/versions/{projectVersionId}/hierarchical-components`

- List hierarchical children components:

```
GET /api/projects/{projectId}/versions/{projectVersionId}/components/  
{componentId}/hierarchical-components/{hierarchicalId}/children
```

- List hierarchical children component versions:

```
GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/  
{componentVersionId}/hierarchical-components/{hierarchicalId}/children
```

- New fields were added to the notifications API for vulnerabilities to enable further classification of notifications. These notifications involve vulnerability information that has changed in a BOM and includes the following fields:

- vulnerabilityNotificationCause

Information about the kind of vulnerability event that occurred and triggered a notification such as a vulnerability was added or removed, changed comment, changed remediation details, changed severity of vulnerability, or the status changed.

- eventSource

Information about the source that generated the notification, such as a scan, Black Duck KB update, or user actions such as remediation, reprioritization, or adjustment.

- The /api/catalog-risk-profile-dashboard API now returns HTTP 410 (GONE).

Supported browser versions

- Safari Version 13.1.2 (14609.3.5.1.5)
- Chrome Version 86.0.4240.80
- Firefox 82 (64-bit)
- Internet Explorer 11.572.19041.0

Note that support for Internet Explorer 11 is deprecated and Synopsys will be ending support for Internet Explorer 11 starting with the Black Duck 2021.2.0 release.

- Microsoft Edge 86.0.622.51 (Official build) (64-bit)

Container versions

- blackducksoftware/blackduck-postgres:1.0.13
- blackducksoftware/blackduck-authentication:2020.10.0
- blackducksoftware/blackduck-webapp:2020.10.0
- blackducksoftware/blackduck-scan:2020.10.0
- blackducksoftware/blackduck-jobrunner:2020.10.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.6
- blackducksoftware/blackduck-registration:2020.10.0
- blackducksoftware/blackduck-nginx:1.0.26

- blackducksoftware/blackduck-documentation:2020.10.0
- blackducksoftware/blackduck-upload-cache:1.0.15
- blackducksoftware/blackduck-redis:2020.10.0
- sigsynopsys/bdba-worker:2020.09
- blackducksoftware/rabbitmq:1.2.2

Japanese language

The 2020.8.0 version of the UI, online help, and release notes has been localized to Japanese.

Fixed Issues in 2020.10.0

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

- (Hub-20559, 22100). Fixed an issue where snippet adjustments were lost when scanning the same code location from a different root directory or when cloning a project version.
- (Hub-21421). Fixed an issue where the print functionality did not work for large projects.
- (Hub-23705, 25560). Fixed an issue where users could not delete reports that they created.
- (Hub-23709). Fixed an issue whereby the following scan.cli.sh warning message appeared when scanning: "Unable to find manifest from all manifests."
- (Hub-24330). Fixed an issue whereby an error message ("Duplicate key value violates unique constraint") appeared when importing a Protex project into Black Duck version 2019.10.3.
- (Hub-24673). Fixed an issue whereby navigating from a Dashboard page failed if there were more than 32,000 components.
- (Hub-24675). Fixed an issue whereby the root_bom_consumer_node_id was set incorrectly
- (Hub-24871). Fixed an issue with PostgreSQL database growth since release 2019.10.0.
- (Hub-24772). Fixed an issue where the default .pdf filename when printing a BOM was not the project name and version name.
- (Hub-24839). Fixed an issue where some component origin IDs could not be selected from the Add/Edit Component dialog box.
- (Hub-24947). Fixed an issue whereby search results when adding a project to a BOM were listed inconsistently.
- (Hub-25171). Fixed an issue whereby the vulnerability count was not updated when remediated using an API until after a rescan (PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/origins/{originId}/vulnerabilities/{vulnerabilityId}/remediation).
- (Hub-25219). Fixed an issue with creating reports through the API, wherein specifying a locale such as "locale" : "ja_JP" was ignored. Now, the locale field correctly sets the language of the generated report.
- (Hub-25234). Fixed an issue where the **Print** button to print a BOM was occasionally missing bar graph counts.
- (Hub-25240). Fixed an issue where browser or API calls for a specific vulnerability (BDSA-2020-1674) failed.
- (Hub-25241). Fixed an issue where the VersionBomComputationJob failed for scans with the

following error message: "Data integrity violation (Constraint:not_null, Detail: on column source_start_lines)".

- (Hub-25244). Fixed an issue whereby manually added components were deleted from the BOM after upgrading to Black Duck release 2020.4.2.
- (Hub-25247). Fixed an issue whereby the following error message appeared in the Black Duck PostgreSQL logs: "ERROR: duplicate key value violates unique constraint "scan_component_scan_id_bdio_node_id_key".
- (Hub-25321). Fixed an issue where when scrolling the BOM page, text appeared in areas on the page where text should not appear.
- (Hub-25324). Fixed an issue where the Scan *Name* page did not word wrap.
- (Hub-25478). Fixed an issue where the security risk filter on the Security page became invisible.
- (Hub-25508). Fixed an issue where old media types (v4 and v5) did not always work for the policy rules API (GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/policy-rules).
- (Hub-25522, 25523). Fixed an issue where formatting issues appeared in the BOM print preview window in Chrome for Black Duck version 2020.8.0.
- (Hub-25548). Fixed an issue where selecting new component matches in the hierarchical view did not update component matches in the Source view.
- (Hub-25570). Fixed an issue whereby the Security Dashboard page only partially loaded.
- (Hub-25608). Fixed an issue where vulnerabilities were counted twice in the "New Vulnerabilities" and "New Remediated Vulnerabilities" categories in the Vulnerability Update report.
- (Hub-25649). Fixed an issue where the policy violation popup windows on the Dashboard page would not close.
- (Hub-25841). Fixed an issue whereby numbers entered into a custom field of type Text were converted into a date format.

Chapter 3: Known Issues and Limitations

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

New Known Issues

Detect Parameter Incompatibility

Please note, customers currently using Blackduck 2021.8.0 or later might experience timeout issues when Detect is invoked with the following parameters in a request:

- `--detect.wait.for.results=true`
- `--min-scan-interval=` (a non-zero, positive value)

This issue will be resolved in an upcoming Detect and Blackduck release.

Current Known Issues and Limitations

- 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.