



Release Notes

Version 2020.10.0



This edition of the *Release Notes* refers to version 2020.10.0 of Black Duck.

This document created or updated on Wednesday, October 28, 2020.

Please send your comments and suggestions to:

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

Copyright © 2020 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 2020.10.0	1
New containers and changes to system requirements postponed to the 2020.12.0 release	1
Japanese language	1
Announcement for Version 2020.8.0	1
Deprecation of PostgreSQL version 9.6 for external databases	1
Deprecated API in 2020.10.0 release	2
Japanese language	2
Announcement for Version 2020.6.1	2
Ending support for Internet Explorer 11	2
Announcement for Version 2020.6.0	2
New containers and changes to system requirements in future releases	2
Deprecating Internet Explorer 11 support	3
PostgreSQL 11 support for external databases	3
Announcement for Version 2020.2.0	4
Individual file matching	4
Docker Compose support	4
Announcement for Version 2019.12.0	4
Upgrading Black Duck	4
Individual File Matching in the upcoming 2020.2.0 release	5
Docker Compose support	6
Announcement for Version 2019.10.0	6
Redesigned Report Database	6
Announcement for Version 2019.8.0	7
Upgrade Announcement for Version 2019.8.0	7
Chapter 2: Release Information	8
Version 2020.10.0	8
New and Changed Features in Version 2020.10.0	8
Fixed Issues in 2020.10.0	13
Version 2020.8.1	15
New and Changed Features in Version 2020.8.1	15
Fixed Issues in 2020.8.1	15
Version 2020.8.0	16

New and Changed Features in Version 2020.8.0	16
Fixed Issues in 2020.8.0	22
Version 2020.6.2	23
New and Changed Features in Version 2020.6.2	23
Fixed Issues in 2020.6.2	23
Version 2020.6.1	23
New and Changed Features in Version 2020.6.1	23
Fixed Issues in 2020.6.1	23
Version 2020.6.0	24
New and Changed Features in Version 2020.6.0	24
Fixed Issues in 2020.6.0	29
Version 2020.4.2	30
New and Changed Features in Version 2020.4.2	30
Fixed Issues in 2020.4.2	30
Version 2020.4.1	30
New and Changed Features in Version 2020.4.1	30
Fixed Issues in 2020.4.1	30
Version 2020.4.0	30
New and Changed Features in Version 2020.4.0	30
Fixed Issues in 2020.4.0	35
Version 2020.2.1	36
New and Changed Features in Version 2020.2.1	36
Fixed Issues in 2020.2.1	36
Version 2020.2.0	37
New and Changed Features in Version 2020.2.0	37
Fixed Issues in 2020.2.0	40
Version 2019.12.1	41
New and Changed Features in Version 2019.12.1	41
Fixed Issues in 2019.12.1	41
Version 2019.12.0	42
New and Changed Features in Version 2019.12.0	42
Fixed Issues in 2019.12.0	45
Version 2019.10.3	46
New and Changed Features in Version 2019.10.3	46
Fixed Issues in 2019.10.3	46
Version 2019.10.2	46
New and Changed Features in Version 2019.10.2	46
Fixed Issues in 2019.10.2	46
Version 2019.10.1	46
New and Changed Features in Version 2019.10.1	46
Fixed Issues in 2019.10.1	46

Version 2019.10.0	47
New and Changed Features in Version 2019.10.0	47
Fixed Issues in 2019.10.0	51
Version 2019.8.1	52
New and Changed Features in Version 2019.8.1	52
Fixed Issues in 2019.8.1	52
Version 2019.8.0	52
New and Changed Features in Version 2019.8.0	52
Fixed Issues in 2019.8.0	55
Version 2019.6.2	56
New and Changed Features in Version 2019.6.2	56
Fixed Issues in 2019.6.2	56
Version 2019.6.1	56
New and Changed Features in Version 2019.6.1	56
Fixed Issues in 2019.6.1	56
Version 2019.6.0	57
New and Changed Features in Version 2019.6.0	57
Fixed Issues in 2019.6.0	60
Chapter 3: Known Issues and Limitations	63

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.
Installing Black Duck using Kubernetes	install_kubernetes.pdf	Contains information about installing and upgrading Black Duck using Kubernetes.
Installing Black Duck using OpenShift	install_openshift.pdf	Contains information about installing and upgrading Black Duck using OpenShift.
Getting Started	getting_started.pdf	Provides first-time users with information on using Black Duck.
Scanning Best Practices	scanning_best_practices.pdf	Provides best practices for scanning.
Getting Started with the SDK	getting_started_sdk.pdf	Contains overview information and a sample use case.
Report Database	report_db.pdf	Contains information on using the report database.
User Guide	user_guide.pdf	Contains information on using Black Duck's UI.

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

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>
- Email: software-integrity-support@synopsys.com
- Phone: See the Contact Us section at the bottom of our [support page](#) to find your local phone number.

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>.

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.

Announcement for Version 2019.12.0

Upgrading Black Duck

During the upgrade process, as part of the changes made to the reporting database, a migration script will run to purge rows that are no longer used in the `audit_event` table. This migration script may take some time to run, depending on the size of the `audit_event` table. As a guide, the migration script ran approximately 20 minutes for an `audit_event` table sized at 350 GB.

⚙️ To determine the size of the audit event table:

Do one of the following:

- From the `bds_hub` database, run the following command:

```
SELECT pg_size_pretty( pg_total_relation_size('st.audit_event') );
```

- Log in to the Black Duck UI with the system administrator role and do the following:

1. Click the expanding menu icon  and select **Administration**.

The Administration page appears.

2. Select **System Administration** to display the System Information page.
3. Select **db** in the left column of the page.
4. Scroll to the **Table Sizes** section. Find the `total_tbl_size` value for the `audit_event` tablename.

For on-premise Kubernetes and OpenShift users, before upgrading, disable the liveness check (`--liveness-probes false`), upgrade Black Duck, and then wait for the user interface to appear. Once the user interface appears, enable the liveness check (`--liveness-probes true`).

After the migration script runs, Synopsys *strongly recommends* running the `VACUUM` command on the `audit_event` table to optimize PostgreSQL performance.

- Depending on your system usage, running the `VACUUM` command can reclaim a significant amount of disk space no longer in use by Black Duck.
- By running this command, querying performance will be improved.

Note: If you do not run the `VACUUM` command, there may be a degradation of performance.

Note that this command requires twice the amount of disk space currently being used by the `audit_event` table.

Important: You must ensure you have enough space to run the `VACUUM` command, otherwise, it will fail by running out of disk space and possibly corrupting the entire database.

⚙️ To run the `VACUUM` command for Docker Compose and Docker Swarm users with containerized PostgreSQL database deployments:

1. Determine the size of the `audit_event` table as previously described.
2. Determine the container ID of the PostgreSQL container by running the following command:

```
docker ps
```

3. Run the following command to manage the PostgreSQL container:

```
docker exec -it <container_ID> psql bds_hub
```

4. Run the following command:

```
VACUUM FULL ANALYZE st.audit_event;
```

For Docker Compose and Docker Swarm users with an external PostgreSQL database deployment: determine the size of your `audit_event` table, execute the `VACUUM` command and, once complete, restart your deployment.

For on-premise Kubernetes and OpenShift users, refer to the Synopsys Operator upgrade instructions for more information.

Individual File Matching in the upcoming 2020.2.0 release

To reduce false positives due to ambiguous matches, starting in Black Duck version 2020.2, performing

individual file matching as a part of signature scanning will no longer be 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 produces a fair amount of false positives. These false positives require you to spend additional effort to review and adjust the BOM. Though some users may desire this level of precision and granularity in their BOMs, a majority of customers do not desire or need this level of matching. Therefore, based upon customer and field input, in order to improve upon the overall developer experience across the broad Synopsys customer base, individual file matching will no longer be the default behavior and instead will become an optional capability.

This may cause some components to drop off your BOM, which may or may not be desired. Therefore, in the Black Duck 2020.2 release, Synopsys will provide mechanisms so that you can re-enable individual file matching, including in the CLI, Synopsys Detect, and Synopsys Detect (Desktop).

Docker Compose support

As of December 31, 2019, Docker Compose is no longer supported.

Announcement for Version 2019.10.0

Redesigned Report Database

The Reporting Database is a capability in Black Duck which allows customers to use third party BI/reporting tools over the data from Black Duck. In order to improve the administration, stability, and functionality of the reporting database, the 2019.10.0 release has made some significant changes to the reporting database. If you use the reporting database, these updates will require action and change on your part in order to have continued, uninterrupted use of the reporting database.

In order to make it easier for you to quickly create, use, back up, and restore your reporting database, the tables from the separate reporting database (`bd_hub_report`) have been moved to the `reporting` schema in the Black Duck database, `bds_hub`, with a default update frequency of every 8 hours (which can be adjusted). In addition, we have also added new information to the reporting database and you can now create reports which include file/directory and package match information as well. As a result of the improvements, if you are using the report database, you will need to change your database connection string for any tools/utilities/queries to point to the `bds_hub` database and no longer use the `bd_hub_report` database. Any reports (or any queries) will fail unless you change the database connection string to point to the `bds_hub` database as the tables in the old database have been dropped.

Please note that after the 2019.10.0 release, there will be a delay for any changes made in Black Duck to appear in the report database. The length of time for this delay depends on the value you specified using the new `BLACKDUCK_REPORTING_DELAY_MINUTES` environment variable, which by default, equals 8 hours. Customers with Black Duck installed on premise can refer to the appropriate install guide for their platform for information on how to change this frequency. Hosted customers should notify Synopsys Support if they would like to change this value.

Announcement for Version 2019.8.0

Upgrade Announcement for Version 2019.8.0

For customers upgrading from a version prior to 2019.8.0, two jobs, the VulnerabilityReprioritizationJob and the VulnerabilitySummaryFetchJob, will run at startup to synchronize vulnerability data.

These jobs may take some time to run and the overall vulnerability score for existing BOMs will not be available until these jobs complete. Users with the System Administrator role can use the Black Duck Jobs page to monitor these jobs.

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

The ComponentDashboardRefreshJob has been removed.

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.

New Signature Scanner parameter

A new parameter **--baseDir <writable dir>** has been added to the Signature Scanner. Use this parameter when the installed scan.cli directory is not writable for the user running the scan.

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-24574). Fixed an issue whereby ComponentDashboardRefreshJob failed with "No Space left on device" error.
- (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-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-24871). Fixed an issue with PostgreSQL database growth since release 2019.10.0.
- (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-25196). Fixed an issue whereby the Signature Scanner would not complete when WRITE permissions were not given to the `scan.cli` directory.
- (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.

Version 2020.8.1

New and Changed Features in Version 2020.8.1

Ability to clean up unmapped code locations by time

Black Duck now gives you the ability to configure a scan purge cron job by setting the `blackduck.scan.processor.scanpurge.cronstring` variable in the `blackduck-config.env` file for Docker Swarm implementations.

Policy enhancement

Black Duck now provides you the ability to create a policy for the remediation status of a vulnerability.

Container versions

- `blackducksoftware/blackduck-postgres:1.0.13`
- `blackducksoftware/blackduck-authentication:2020.8.1`
- `blackducksoftware/blackduck-webapp:2020.8.1`
- `blackducksoftware/blackduck-scan:2020.8.1`
- `blackducksoftware/blackduck-jobrunner:2020.8.1`
- `blackducksoftware/blackduck-cfssl:1.0.1`
- `blackducksoftware/blackduck-logstash:1.0.6`
- `blackducksoftware/blackduck-registration:2020.8.1`
- `blackducksoftware/blackduck-nginx:1.0.25`
- `blackducksoftware/blackduck-documentation:2020.8.1`
- `blackducksoftware/blackduck-upload-cache:1.0.15`
- `blackducksoftware/blackduck-redis:2020.8.1`
- `sigsynopsys/bdba-worker:2020.06-2`
- `blackducksoftware/rabbitmq:1.2.1`

Fixed Issues in 2020.8.1

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

- (Hub-24149). Fixed an issue with the Protex BOM Tool which displayed an "ERROR StatusLogger Unrecognized..." error message regardless of the operation performed.
- (Hub-24480). Fixed an issue whereby components imported from Protex lost their ignored status when Black Duck was upgraded to version 2020.4.1.
- (Hub-25254). Fixed an issue where a policy violation was incorrectly triggered after the distribution type was changed.
- (Hub-25269, 25416). Fixed an issue whereby a long running query was blocking scans or causing a

deadlock in the PostgreSQL database.

- (Hub-25387). Fixed an issue whereby the KbUpdateJob was intermittently failing.
- (Hub-25509). Fixed an issue with the rapid increase in the size of the database in Black Duck version 2020.4.2.

Version 2020.8.0

New and Changed Features in Version 2020.8.0

Ability to analyze the impact of a vulnerability

To help you to prioritize which vulnerabilities you should address first, Black Duck can now determine if any external public methods called by your Java applications are potentially involved in a known vulnerability. Black Duck can identify the called fully qualified public functional names in your source code and match them to the known function names being exploited by a vulnerability. By knowing whether any external public methods called by your Java applications are potentially involved in a known vulnerability, you can prioritize what vulnerabilities you need to concentrate on.

This feature is available in Synopsys Detect version 6.5 or later (and Synopsys Detect (Desktop) that uses Synopsys Detect 6.5 and later) for Java applications only.

Note the following:

- Synopsys Detect only discovers vulnerabilities in Java public methods that call potentially vulnerable functions.
- This feature displays reachable functions for BDSAs only.

New container and system requirements

A new Redis container has been added to Black Duck. This container enables more consistent caching functionality in Black Duck and will improve application performance.

The minimum hardware needed to run a single instance of all containers is now:

- 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 minimum hardware needed to run Black Duck with Black Duck - Binary Analysis is now:

- 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.

Custom system announcements

System Administrators can now create custom sign-on and post sign-on messages to your Black Duck users.

For example, use system announcements to tell your users about upcoming events or if you need to show a disclaimer indicating what happens for unauthorized use.

There are four types of messages that you can create:

- Login. A message that appears to the user when they are logging in to Black Duck.
- Banner. A message that appears at the top of every page.
- Footer. A message that appears in the footer of every page.
- Welcome. A message that appears after the user logs in to Black Duck.

Enhancements to project version reports

New upgrade guidance project version report

A new report, `project_version_upgrade_guidance_date_time.csv`, has been added to the project version reports.

This report includes:

- component version details, including origin information and total vulnerabilities
- short term upgrade guidance for the component (if any), including the version/origin to upgrade to and its details such as total vulnerabilities
- long term upgrade guidance for the component (if any), including the version/origin to upgrade to and its details such as total vulnerabilities

Columns in this report are:

- Component Id
- Component Version Id
- Component Origin Id
- Component Name
- Component Version Name
- Component Origin Name
- Component Origin Id
- Component Origin Version Name
- Total Known Vulnerabilities
- Short Term Recommended Version Id
- Short Term Recommended Version Name
- Short Term Recommended Component Origin Id
- Short Term Recommended Origin Name

- Short Term Recommended Origin Id
- Short Term Recommended Origin Version Name
- Short Term Critical Vulnerability
- Short Term Critical High Vulnerability
- Short Term Medium Vulnerability
- Short Term Low Vulnerability
- Long Term Recommended Version Id
- Long Term Recommended Version Name
- Long Term Recommended Component Origin Id
- Long Term Recommended Origin Name
- Long Term Recommended Origin Id
- Long Term Recommended Origin Version Name
- Long Term Critical Vulnerability
- Long Term High Vulnerability
- Long Term Medium Vulnerability
- Long Term Low Vulnerability

New columns added to the `security_date_time.csv` report

These new columns have been added to the end of the `security_date_time.csv` project version report:

- CVSS Version. Version of the vulnerability scoring system: CVSS 2.0 or CVSS 3.x.
- Match type.

Enhancements to the Signature Scanner

Two new properties have been added to the Signature Scanner to control how scan data is streamed (buffered) from the Signature Scanner to Black Duck. In rare cases, you may need to modify these values to better suit your network, for example, decreasing the values if there are issues with your network or increasing the default values if your network is highly stable.

- **-max-request-body-size**. Size of the main request that uploads the scan data for scanned paths.
- **-max-update-size** Buffers an update request to inform Black Duck when the Signature Scanner has completed uploading the data of individual URLs (scanned paths).

API enhancements

- Provide the last login date for a specific Black Duck user.

GET `/api/users/{userId}/last-login`

Upon upgrade to 2020.8.0, the last login date for all users defaults to the upgrade date but after that uses the actual login data. By default, this endpoint will show all users who have not logged in the past 30 days, but you can add a `?sinceDays=` query parameter to change the lookback period to any number of days required. This will also show users who have been created but never logged into the system.

- Find dormant users.

GET /api/dormant-users

■ Added the following endpoints for announcements:

- Create login announcement.

POST /api/manage-announcement/login

- Create welcome announcement.

POST /api/manage-announcement/welcome

- Create banner announcement.

POST /api/manage-announcement/banner

- Create footer announcement.

POST /api/manage-announcement/footer

- Edit login announcement.

PUT /api/manage-announcement/login/{announcementId}

- Edit welcome announcement.

PUT /api/manage-announcement/welcome/{announcementId}

- Edit banner announcement.

PUT /api/manage-announcement/banner/{announcementId}

- Edit footer announcement.

PUT /api/manage-announcement/footer/{announcementId}

- Delete login announcement.

DELETE /api/manage-announcement/login/{announcementId}

- Delete welcome announcement.

DELETE /api/manage-announcement/welcome/{announcementId}

- Delete banner announcement.

DELETE /api/manage-announcement/banner/{announcementId}

- Delete footer announcement.

DELETE /api/manage-announcement/footer/{announcementId}

- Get login announcement.

GET /api/manage-announcement/login

- Get welcome announcement.
GET /api/manage-announcement/welcome
- Get banner announcement.
GET /api/manage-announcement/banner
- Get footer announcement.
GET /api/manage-announcement/footer
- Get login announcement by ID.
GET /api/manage-announcement/login/{announcementId}
- Get welcome announcement by ID.
GET /api/manage-announcement/welcome/{announcementId}
- Get banner announcement by ID.
GET /api/manage-announcement/banner/{announcementId}
- Get footer announcement by ID.
GET /api/manage-announcement/footer/{announcementId}
- Get user login announcement.
GET /api/announcement/login
- Get user welcome announcement.
GET /api/announcement/welcome
- Get user banner announcement.
GET /api/announcement/banner
- Get user footer announcement.
GET /api/announcement/footer
- Get user login announcement by ID.
GET /api/announcement/login/{announcementId}
- Get user welcome announcement by ID.
GET /api/announcement/welcome/{announcementId}
- Get user banner announcement by ID.
GET /api/announcement/banner/{announcementId}

- Get user footer announcement by ID.

GET /api/announcement/footer/{announcementId}

- Suppress welcome announcement.

POST /api/announcement/welcome/{announcementId}/suppress

- Added new optional originUrl field for API origin responses.
- Added a BOM API (api/projects/id/versions/id/components) reference to api/projects/id/versions/id/references.
- Added createdByUserName in the response for api/codelocations/id/scan-summaries.
- Added componentType field to /api/projects/versions/hierarchical-components and if an item's componentType is SUB_PROJECT it will also have project and projectVersion links in its metadata.
- Added relatedVulnerability link under the vulnerabilityWithRemediation block to /api/projects/{projectId}/versions/{projectVersionId}/vulnerable-bom-components.
- Added remediationCreatedBy and remediationUpdatedBy to /api/projects/{projectId}/versions/{projectVersionId}/vulnerable-bom-components
- Deprecated endpoint:
 - Listing remediation options: GET /api/components/{componentId}/versions/{componentVersionId}/remediating.

This endpoint has been replaced by GET /api/components/{componentId}/versions/{componentVersionId}/upgrade-guidance.

Supported browser versions

- Safari Version 13.1.2 (14609.3.5.1.5)
- Chrome Version 84.0.4147.125 (Official Build) (64-bit)
- Firefox 79.0 (64-bit)
- Internet Explorer 11.450.19041.0

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 44.19041.423.0
- Microsoft EdgeHTML 18.19041

Container versions

- blackducksoftware/blackduck-postgres:1.0.13
- blackducksoftware/blackduck-authentication:2020.8.0
- blackducksoftware/blackduck-webapp:2020.8.0
- blackducksoftware/blackduck-scan:2020.8.0
- blackducksoftware/blackduck-jobrunner:2020.8.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.6

- blackducksoftware/blackduck-registration:2020.8.0
- blackducksoftware/blackduck-nginx:1.0.25
- blackducksoftware/blackduck-documentation:2020.8.0
- blackducksoftware/blackduck-upload-cache:1.0.15
- blackducksoftware/blackduck-redis:2020.8.0
- sigsynopsys/bdba-worker:2020.03-1
- blackducksoftware/rabbitmq:1.2.1

Japanese language

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

Fixed Issues in 2020.8.0

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

- (Hub-23467). Fixed an issue where the Scan page displayed a "Server did not respond in time" error message when there are more than 1,300 matches.
- (Hub-23892). Fixed an issue whereby the **Scan Size** column was empty on the Scans page.
- (Hub-23937, 24799). Fixed an issue where the License Management page failed to load.
- (Hub-24009). Fixed an issue whereby the bom-import failed intermittently with a 400 code in the Synopsys Detect output and the `hub_scan_errors.log` listed "Failed saving document data for document null".
- (Hub-24112). Fixed an issue so that users can now return to the match count filter view when a node is no longer selected on the project version **Source** tab.
- (Hub-24278). Fixed an issue where the binary scan file failed to upload with the following error message: Unknown status code when uploading binary scan: 0, null.
- (Hub-24291). Fixed an issue whereby the BOM page displayed "The application has encountered an unknown error" when attempting to display more than 32,767 components.
- (Hub-24407). Fixed an issue whereby the error message "Unable to deserialize from string" appeared when cloning snippets.
- (Hub-24432). Fixed an issue whereby the Dashboard page would not load when attempting to display more than 32,000 projects.
- (Hub-24451). Fixed an issue whereby HUB_PROXY_PASSWORD_FILE docker secret was ignored on calls to the Black Duck KnowledgeBase using an authenticating proxy.
- (Hub-24480). Fixed an issue whereby component modifications were lost when importing Protex into Black Duck 2020.4.1.
- (Hub-24529). Fixed an issue whereby policy violations were incorrectly triggered for components with a patched status as denoted by the Black Duck KnowledgeBase.
- (Hub-24583, 25244). Fixed an issue whereby manually added components were deleted when the Black Duck KnowledgeBase was updated.
- (Hub-24646). Fixed an issue which occurred upon upgrading Black Duck where a KnowledgeBase license was updated on the License Management page, however, no user was identified as making the change.
- (Hub-24673). Fixed an issue when navigating from the Dashboard page to the Components page failed if there are more than 32,000 components.

- (Hub-24716). Fixed an issue whereby a vulnerability notification appeared for ignored components.
- (Hub-24739). Fixed an issue whereby the LDAP users' email addresses could not be modified.
- (Hub-24740). Fixed an issue whereby the `bom_component_custom_fields_date_time.csv` report showed ignored components only.
- (Hub-24758). Fixed an issue whereby the side-by-side snippet view did not completely highlight the matched code on the left side of the project version **Source** tab.
- (Hub-24845). Fixed an issue whereby the **Statistic** section in the **Summary** tab was not updated.
- (Hub-24866). Fixed an issue whereby the Signature Scanner reported a Bad Request error when attempting to scan an entire root on a disk while excluding some of the root's subdirectories.
- (Hub-24885). Fixed an issue whereby attempting to view matches in the project version **Source** tab from the hierarchical view resulted in 'The application has encountered an unknown error' message.
- (Hub-24968). Fixed an issue whereby the following error message "The Black Duck server did not respond in time." appeared when attempting to view the Security Dashboard.
- (Hub-25072). Fixed an issue whereby "The application has encountered an unknown error." error message appeared when creating a policy for a component with a tilde (~) character in its name.
- (Hub-25115). Fixed an issue where scanning failed if there were more than 32,767 parameters.
- (Hub-25166). Fixed an issue and added a pre- and post- command to fix a postgres-init pod in an Istio environment.

Version 2020.6.2

New and Changed Features in Version 2020.6.2

Black Duck version 2020.6.2 is a maintenance release and contains no new or changed features.

Fixed Issues in 2020.6.2

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

- (Hub-24918). Fixed an issue where scanning did not consistently return results as the `BdioDataTransferJob` and `VersionBomComputation` jobs were not reading scan data correctly.

Version 2020.6.1

New and Changed Features in Version 2020.6.1

Black Duck version 2020.6.1 is a maintenance release and contains no new or changed features.

Fixed Issues in 2020.6.1

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

- (Hub-23970). Fixed an issue whereby the notices file could not be generated if the copyright option was selected.
- (Hub-24106). Fixed an issue where the `KbUpdate` Job failed as the KnowledgeBase service could not be accessed.
- (Hub-24651). Fixed an issue whereby a user with the Project Manager and BOM Manager roles could not

use the release phase filter on the /api/projects/ page.

- (Hub-24721). Fixed an issue whereby the BOM component report failed when Black Duck Security Advisories (BDSA) was not a licensed module.
- (Hub-24739). Fixed an issue whereby LDAP users' email addresses could not be modified.
- (Hub-24765). Fixed an issue whereby snippets were not always identified when scanned using the SNIPPET_MATCHING option.

Version 2020.6.0

New and Changed Features in Version 2020.6.0

New Project Dashboard with saved searches

Black Duck provides dashboards so that you can view the types and severity of risk and policy violations that are associated with the components that are in one or more versions of your projects. Dashboards provide an overall view across all of your projects and project versions.

So that you can view the projects and project versions that are important to you, in 2020.6.0, the Project Dashboard has been replaced with two new default dashboards and the ability for you to create an unlimited number of custom dashboards.

Black Duck displays these two default dashboards:

- **Watching**. Your watched projects.
- **My Projects**. All of your projects, including projects that you are not watching.

These dashboards display information on the new Dashboard page at the project level. This Dashboard page replaces the Project Dashboard page.

In addition, you can create custom dashboards so that you can quickly view the project versions that are important to you. Black Duck now provides the ability for you to search for projects using a variety of attributes, save the search, and then use this page to view dashboards from those saved searches. Dashboards based on saved searches display information at the project version level.

The information shown for the **Watching** and **My Projects** dashboards is updated in real time. A new job, SearchDashboardRefreshJob, refreshes your custom dashboards every five minutes.



Click  to display the dashboards. If not displayed, select **Dashboard** to display these dashboards.

Project search enhancements

Searching for projects has been enhanced by the attributes you can use to search for the project and the information shown in the search results.

You can now search for projects in Black Duck using the following attributes:

- **Watching**. Select whether this project is a watched project.
- **Security Risk**.
- **License Risk**.

- Operational Risk.
- Policy Rule. Select a policy rule from the list to find the projects that violate this policy.
- Policy Violation. Severity level of the policy rule.
- Distribution.
- Last Scanned Date.
- Release Phase.
- Tier.

Search results show the project versions that meets your search criteria. For each project version, you can view the number of:

- Results found and the time the database was last updated.
- Components with the highest level of security, license, or operational risk.
- Components for each risk category.
- Components with the highest policy severity level for this project version.
- Components with policy violations by severity level.

For each project version, the search results also show:

- Number of components in this project version.
- Last scan date.
- When this project version was last updated.
- License of this project version.
- Phase for this project version.
- Distribution of this project version.

Search results can now be saved and view in the Dashboard, as described previously.

Embedded copyright statement detection

Black Duck can now detect instances of embedded copyright statements. By enabling detection of copyright data when scanning code, users focused on license compliance can reduce license compliance risks by detecting and managing open source software and proprietary copyrights statements.

With this feature, Black Duck performs a search for copyright string text and displays the text found in the **Source** tab.

Optionally, upload your source files so that reviewers can view discovered copyright text in the file from within the **Source** tab.

Cloning projects

Black Duck now provides you the ability to clone projects. Use project cloning to fork an existing project to a new project. Cloning helps reduce your workload by using the data, analysis, and resolutions you defined in an existing project as a baseline for a new project.

Users who can create projects can clone projects. For each project, select the versions you wish to clone and the project's attributes, such as the project's settings or project members and groups.

Policy management enhancements

- Policy management now provides the ability to create policy rules based on:
 - License expiration date
 - BOM component custom fields for Boolean, Date, Drop Down, Multiple Selections, Single Selection, and Text field types.
 - Project filters now includes project custom fields for Boolean, Multiple Selections, and Text field types.
- The logic for evaluating license policy conditions for components with multiple licenses has been modified, which may result in new policy violations or components no longer triggering a policy violation:

When evaluating components with multiple licenses for policy rules created using one or more of these license conditions: license, license status, license family and/or license expiration date, each license is evaluated and *all* license conditions must be true for a policy violation. If license risk is included as a policy condition, license risk is evaluated independently: all licenses for the component are evaluated, not just the license that met the other license policy conditions. Therefore, a policy violation can be triggered if one license meets the policy rule for multiple conditions while another license for that component meets the license risk condition.

PostgreSQL 11.7 supported 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.

Numeric usernames supported for external PostgreSQL databases

External PostgreSQL instances now support usernames that consist of only numeric characters.

Notices File report enhancements

Licenses in the Unknown licenses family are now excluded from the Notices File report.

Global vulnerability reports now available for individual projects

The Vulnerability Remediation report, Vulnerability Status report, and Vulnerability Update report can now be run for one or more projects to which you have access,

To differentiate whether a report is at the global or project level, the file name for these reports have been modified to:

- vulnerability-remedation-report_all_assigned_projects_YYYY-MM-DD_HHMMSS (time stamp in UTC) for a global version of the report
- vulnerability-remedation-report_YYYY-MM-DD_HHMMSS (time stamp in UTC) for one or more projects
- vulnerability-status-report_all_assigned_projects_YYYY-MM-DD_HHMMSS (time stamp in UTC) for a global version of the report
- vulnerability-status-report_YYYY-MM-DD_HHMMSS (time stamp in UTC) for one or more projects

- vulnerability-update-report_all_assigned_projects_YYYY-MM-DD_HHMMSS (time stamp in UTC) for a global version of the report
- vulnerability-update-report_YYYY-MM-DD_HHMMSS (time stamp in UTC) for one or more projects

Additional information added to the source project version report

The `source_date_time.csv` report has been enhanced with the following information:

- The Scan column has been added to the end of the report. As a project version BOM can have multiple scans mapped to a project version, this column lists the scan where this match was found.
- The Path column now displays information for dependency matches. For a direct dependency, the column shows the ID of the dependency and displays the match content value. For transitive dependencies, the column shows the full dependency path from the top level component to the declared component.

Support for CVSS v3.1

Black Duck now supports CVSS v3.1 scores. CVSS v3.1 is an update to the scoring standard which clarifies how scoring is performed. While no new metric vectors or values were created, overall scores may change based upon the clarification.

Reporting database enhancements

The following columns have been added to the component_vulnerability table to support CVSS 3.x:

- severity_cvss3
- base_score_cvss3
- exploit_score_cvss3
- impact_score_cvss3
- temporal_score_cvss3

Option to retain partial snippet adjustments when rescanning


Black Duck now provides a setting so that you can apply identifications from partial snippet matches when rescanning files. This minimize the number of snippet matches you need to re-identify.

New audit events

An audit event will now appear when a user:

- Creates a policy and Black Duck evaluates a project version.
- Updates a policy and Black Duck evaluates a project version.
- Enables a policy and Black Duck evaluates a project version.
- Disables a policy and Black Duck clears the corresponding policy violations.
- Deletes a policy and Black Duck clears the corresponding policy violations.

New information icon on BOM page

The BOM page now uses the information icon () to indicate whether there is an adjustment or custom field additional information.

- Hover over the icon indicates whether there is an adjustment or there are additional fields.
- Select the icon to open the Component Details dialog box which displays additional information.

API enhancements

- Added a new endpoint to provide a list of component import events that occurs during a matching operation.

GET /api/bom-import/{graphId}/component-import-events

- Added a new endpoint to provide a count of component import events (by status) that occurs during a matching operation.

GET /api/bom-import/{graphId}/component-import-events-count

- Added an API to find out which scan a BOM belongs to, which provides a list of entries discovered by the associated scan.

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

- Added support for copyright search and a new filter was added for copyright search for the Source view API.

- Improved the latest-scan summary API

GET /api/codelocations/{codeLocationId}/latest-scan-summary

Supported browser versions

- Safari Version 13.1.1 (14609.2.9.1.3)
- Chrome Version 83.0.4103.97 (Official Build) (64-bit)
- Firefox 77.0.1 (64-bit)
- Internet Explorer 11.836.18362.0
- Microsoft Edge 44.18362.449.0

Container versions

- blackducksoftware/blackduck-postgres:1.0.13
- blackducksoftware/blackduck-authentication:2020.6.0
- blackducksoftware/blackduck-webapp:2020.6.0
- blackducksoftware/blackduck-scan:2020.6.0
- blackducksoftware/blackduck-jobrunner:2020.6.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.6
- blackducksoftware/blackduck-registration:2020.6.0
- blackducksoftware/blackduck-nginx:1.0.25
- blackducksoftware/blackduck-documentation:2020.6.0
- blackducksoftware/blackduck-upload-cache:1.0.14

- sigsynopsys/bdba-worker:2020.03-1
- blackducksoftware/rabbitmq:1.0.3

Japanese language

The 2020.4.0 version of the UI, online help, and release notes has been localized to Japanese.

Fixed Issues in 2020.6.0

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

- (Hub-20003) Fixed an issue so that the Add Component dialog box now identifies custom components.
- (Hub-22599) Fixed an issue whereby the UI timed out when cloning a project version.
- (Hub-22695) Fixed an issue whereby manually identified components were missing after cloning a project version and rescanning.
- (HUB-22812) Fixed an issue where filters were ignored when printing a BOM.
- (HUB-23502) Fixed an issue where Black Duck deployed on Openshift native mode without the --certificate-file-path parameter did not generate the 'subject alternative names' in certificates.
- (HUB-23601) Fixed an issue so that the **Owners** drop-down menu on the *Project Name Settings* tab displayed all possible selections.
- (HUB-23736) Fixed an issue whereby the HierarchicalVersionBomJob did not run successfully.
- (HUB-23798) Fixed an issue where a 404 error appeared when editing subprojects as a component from the Component dashboard.
- (HUB-23909, 23925) Fixed an issue where the project version **Security** tab did not provide the ability to view vulnerabilities regardless of their status.
- (Hub-23984) Fixed an issue wherein all projects were returned for the GET /api/projects endpoint for a user with no roles assigned.
- (Hub-23985) Fixed an issue whereby selecting a match or using the "Reveal In File Tree" option did not scroll to the file in the source tree.
- (Hub-23994) Fixed an issue whereby Black Duck - Binary Analysis did not clean up uploaded binary files.
- (Hub-24011) Fixed an issue whereby a "413 Request Entity Too Large" error message appeared for a snippet scan.
- (Hub-24040) Fixed an issue whereby the jobrunner hung and jobs did not complete.
- (Hub-24097) Fixed an issue where edits made to usage were not preserved after updating the component version.
- (Hub-24107) Fixed an issue where the Notices File report failed with too many parameters when the copyright option was selected.
- (Hub-24239) Fixed an issue where the api/projects/<projectid>/versions/<versionid>/policy-status displayed a 400 error.
- (Hub-24286) Fixed an issue where soft deleted component versions still appeared in the *Component Name Version* page.
- (Hub-24308) Fixed an issue whereby an empty subproject displayed "componentCount Component" as the source on the BOM page.

Version 2020.4.2

New and Changed Features in Version 2020.4.2

Container Version

- sigsynopsys/bdba-worker:2020.03-1

Fixed Issues in 2020.4.2

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

- (Hub-22837). Fixed an issue whereby not all components in project version BOMs were not being updated with new vulnerability data.
- (Hub-23581). Fixed an issue whereby the webapp container kept restarting.
- (Hub-23869). Fixed an issue where embedded license search results were not displayed when snippet scanning was enabled unless the upload source option was also enabled.
- (Hub-24006). Fixed an issue whereby using the License Management page to update licenses with a large number of components caused the webapp container to crash.

Version 2020.4.1

New and Changed Features in Version 2020.4.1

Black Duck version 2020.4.1 incorporates scanning improvements.

Fixed Issues in 2020.4.1

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

- (Hub-22188). Fixed an issue whereby a scan failed with the error message "Parent of <path> does not exist."
- (Hub-22251). Fixed an issue with scan failures due to Black Duck KnowledgeBase communication issues. To help prevent communication issues, retries of Black Duck KnowledgeBase communication with the Black Duck server are now in incremental intervals.
- (Hub-22559). Fixed an issue whereby the scans remain in the post-scan phase, but the results uploaded successfully to Black Duck.
- (Hub-23465). Fixed an issue with a slow UPDATE scan_composite_leaf query for large projects

Version 2020.4.0

New and Changed Features in Version 2020.4.0

Enhanced management of copyright statements

Users with the new global Copyright Editor role can now easily manage open source copyright statements for their organization so that the full list of copyright holders can be included in your notices file report.

Users with the Copyright Editor role can:

- View all copyright statements for a component version.
- Create or edit custom copyright statements.
- Edit Black Duck KnowledgeBase copyright statements
- Revert an edited Black Duck KnowledgeBase copyright statement to its original text.
- Activate or deactivate copyright statements.

Black Duck manages copyright statements by the origin name/id for a component version. Therefore, edits made to copyright statements for an origin for a component version apply to all BOMs that use that component version origin. This enables you to reuse data across your organization and reduce your workload.

Global remediation status

Black Duck now provides the ability for users with the new Global Security Manager role to set a global default remediation status for security vulnerabilities. After you set a global remediation status, when that vulnerability appears in new BOMs, it will automatically get the global remediation status you defined.

So that you can easily find globally remediated vulnerabilities, there is now a **Default Remediation Status** filter on the Security Dashboard.

Policy categories

Black Duck now provides categories which you can now use to group your policies. Using a new category filter provided on the Policy Management page and on the BOM page, this feature makes it easy for you to find policies (on the Policy Management page) or policy violations (on the BOM page) by category.

Possible categories are component, security, license, operational, and uncategorized (which is the default value).

All policies created prior to the 2020.4.0 release are grouped in the uncategorized category.

Reporting database enhancements

New columns have been added to these tables in the reporting database:

- Component table
 - review_status
 - reviewed_by
 - security_critical_count
 - security_high_count
 - security_medium_count
 - security_low_count
 - security_ok_count
 - license_high_count
 - license_medium_count
 - license_low_count
 - license_ok_count
 - operational_high_count

- operational_medium_count
- operational_low_count
- operational_ok_count
- Component policy table
 - overridden_at
 - description
 - severity
- Component vulnerability table
 - temporal_score
 - attack_vector
 - solution_available
 - workaround_available
 - published_on
 - updated_on
- Project table
 - created_at
- Project version table
 - created_on
 - updated_at
 - security_critical_component_count
 - security_high_component_count
 - security_medium_component_count
 - security_low_component_count
 - security_ok_component_count
 - license_high_component_count
 - license_medium_component_count
 - license_low_component_count
 - license_ok_component_count
 - operational_high_component_count
 - operational_medium_component_count
 - operational_low_component_count
 - operational_ok_component_count

A new view has also been added to the `reporting` schema of `bds_hub` for component comments.

The reporting database uses materialized views. As Excel does not support materialized views, using Excel with the reporting database is no longer supported. Therefore, the documentation for using Excel has been removed from the *Report Database* guide.

Bulk remediation by origin

To make it easier to perform bulk remediation on the vulnerabilities of a single component with multiple origin

IDs, the **Affected Projects** tab for the BDSA and CVE record has been enhanced to display the origins used in each project version.

Remediation guidance

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

This feature is no longer a beta feature and is now available to all customers.

Ability to disable creation of users upon successful LDAP and SAML authentication

Black Duck now provides the ability to disable the automatic creation of users upon successful LDAP or SAML authentication.

Enhancements to custom fields

Black Duck now provides the ability to add new or edit existing options for the dropdown, single, and multiple selection custom fields.

New jobs

These jobs have been added to Black Duck:

- JobMaintenanceJob, which manages data retention and cleanup for existing jobs.
- NotificationPurgeJob, which manages data retention for existing notifications.
- ReportPurgeJob, which manages data retention for existing reports.
- SystemMaintenanceJob, which maintains system-related activities.

API enhancements

- Added the logo or primary language fields for the custom components API.
- Added the critical risk priority that shows critical risks if using CVSS 3 scoring to the /api/components endpoint.
- Added the capability for remediation comments to /api/projects/:projectId/versions/:versionId/vulnerable-bom-components
- Added a "migrated" flag to component and version responses in the response body when the source IDs differ from the retrieved IDs that are returned from the KnowledgeBase.
- Added a public API for the latest scan summary: /api/codelocations/:codeLocationId/latest-scan-summary
- Added a new field to the following endpoint: GET /api/projects/{projectId}/versions/{projectVersionId}/components to show a component type for each entry, such as KB_COMPONENT, CUSTOM_COMPONENT, or SUB_PROJECT.

Removal of the zookeeper container

The zookeeper container has been removed.

- After upgrading to 2020.04.0, you can manually remove the following volumes as they are no longer used and nothing references them:
 - zookeeper-data-volume
 - zookeeper-datalog-volume

- The jobrunner API is deprecated.

You should not develop new queries using this API as it will be removed and replaced in a future release.

- If you used the `terminateJob` function of the Jobs API to terminate a job, it will now always return `false` when called.

Jobs currently cannot be cancelled. This functionality will be re-implemented using a different mechanism in a future release.

Container versions

- blackducksoftware/blackduck-postgres:1.0.13
- blackducksoftware/blackduck-authentication:2020.4.0
- blackducksoftware/blackduck-webapp:2020.4.0
- blackducksoftware/blackduck-scan:2020.4.0
- blackducksoftware/blackduck-jobrunner:2020.4.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.6
- blackducksoftware/blackduck-registration:2020.4.0
- blackducksoftware/blackduck-nginx:1.0.23
- blackducksoftware/blackduck-documentation:2020.4.0
- blackducksoftware/blackduck-upload-cache:1.0.13
- sigsynopsys/bdba-worker:2020.03
- blackducksoftware/rabbitmq:1.0.3

Note that the container `sigsynopsys/appcheck-worker-<version>` has been renamed to `sigsynopsys/bdba-worker-<version>`.

Removal of the bdio database

As mentioned in the 2019.10.0 release notes, the bdio database has now been completely removed from Black Duck .

Changes to the `external-postgres-init.pgsql` initialization file for external PostgreSQL

The `external-postgres-init.pgsql` initialization file was modified to make it more compatible with other deployment methods such as Kubernetes.

When you configure an external PostgreSQL instance, you must edit the `external-postgres-init.pgsql` file in the `docker-swarm` directory and do the following:

- Replace POSTGRES_USER with blackduck
- Replace HUB_POSTGRES_USER with blackduck_user
- Replace BLACKDUCK_USER_PASSWORD with the password that you use for blackduck_user

Using synopsysctl to install or upgrade Black Duck using Kubernetes or OpenShift

As of the 2020.4.0 release, synopsysctl is now the recommended method to install or upgrade Black Duck using Kubernetes or OpenShift.

This change enables Synopsys to include a broader range of Black Duck product enhancements in future releases, while retaining full functionality to manage the applications in your cluster.

Click [here](#) for more information on synopsysctl.

Supported browser versions

- Safari Version 13.1 (14609.1.20.111.8)
- Chrome Version 80.0.3987.162 (Official Build) (64-bit)
- Firefox Version 74.0 (64-bit)
- Internet Explorer 11.657.18362.0
- Microsoft Edge 44.18362.449.0
- Microsoft EdgeHTML 18.18363

Japanese language

The 2020.2.0 version of the UI, online help, and release notes has been localized to Japanese.

Fixed Issues in 2020.4.0

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

- (Hub-15549). Fixed an issue whereby the policy rule filter in the BOM displayed disabled policies.
- (Hub-19745). Incorporated Content Security Protocols (CSP) in HTTP headers.
- (Hub-21044). Fixed snippet matching to ignore false positive matches to import and include statements.
- (Hub-21299). A new **Upload Scans** button was added to the project version **Settings** tab so that a user with only the project code scanner role could upload scans without viewing information that the user does not have permission to see.
- (Hub-21395). Fixed an issue whereby the scan size of bz2 files was not calculated correctly.
- (Hub-22187). Fixed an issue whereby inactive group roles were displayed for the user on the My Profile page.
- (Hub-22609). Fixed an issue whereby the scan failed when scanning an OVA file with BDBA.
- (Hub-22657). Fixed an issue whereby the Signature Scanner CLI displayed "ERROR StatusLogger..." error messages.
- (Hub-22675). Fixed an issue whereby the `crypto_date_time.csv` file reported the incorrect value in the "In Use" column.
- (Hub-22692). Fixed an issue whereby a notification was not received when a scan exceeded the license limit.

- (Hub-22753). Fixed an issue whereby notifications were not being pruned correctly.
- (Hub-22852). Fixed an issue whereby deep license data search did not show the source code of certain file types.
- (Hub-22937). Fixed an issue whereby incorrect search results appeared for a related vulnerability.
- (Hub-22988). Fixed an issue whereby the Where Used value shown for a license in License Management displayed an incorrect number of components for components that did not have any versions.
- (Hub-23097). Fixed an issue whereby the policy override information displayed the incorrect reviewer after the project version was cloned.
- (Hub-23139). Fixed an issue whereby the user could not open the Vulnerability Update report in HTML format.
- (Hub-23175). Fixed an issue whereby selecting a component version link in the Search results never loaded the page.
- (Hub-23217). A message now appears on the BOM page indicating when the BOM is being rebuilt.
- (Hub-23237). Fixed an issue whereby the "Error: cannot accumulate arrays of different dimensionality" error message appeared when accessing the project version.
- (Hub-23258). Fixed an issue whereby an audit_event caused blocked queries and timeouts.
- (Hub-23296). Fixed an issue whereby policy violations for licenses were not triggered when deep license data was enabled.
- (Hub-23306). Fixed an issue whereby paging was broken for the endpoint api/search/components.
- (Hub-23333). Fixed an issue whereby the tooltip did not show the file path for transitive dependencies.
- (Hub-23378). Fixed an issue whereby running more than one instance of Synopsys Detect with the Signature Scanner enabled caused the scan to fail with the following error: "ERROR: zip END header not found".
- (Hub-23523). Fixed an issue whereby the ReportingDatabaseTransferJob failed with an error stating that a key was duplicated.
- (Hub-23602). Fixed an issue whereby a user with the project manager role did not have permission to view the origin ID information in the Reference Files dialog box when viewing deep license data.
- (Hub-23845). Fixed an issue whereby Internet Explorer 11 was not compatible with Black Duck.

Version 2020.2.1

New and Changed Features in Version 2020.2.1

Improved embedded license search performance

Black Duck has improved performance when uploading source files for embedded license detection.

Fixed Issues in 2020.2.1

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

- (Hub-22325). Fixed an issue whereby Black Duck snippet scanning failed if an empty folder was scanned.
- (HUB-22955). Fixed an issue whereby the KBComponentUpdateJob failed with the following error: No object exists with that ID.

- (Hub-22982). Fixed an issue whereby in the BOM page, the component count for security vulnerabilities was inconsistent with how values were calculated in previous versions of Black Duck.

Version 2020.2.0

New and Changed Features in Version 2020.2.0

Individual file matching

Individual file matching as a part of signature scanning is no longer the default behavior for the Black Duck CLI and Synopsys Detect scans.

This change may cause some components to drop off your BOM, which may or may not be desired. Therefore, in the Black Duck 2020.2.0 release, you can re-enable individual file matching.

The Signature Scanner has a new parameter **--individualFileMatching** which has three options so that you can enable individual file matching:

- **source**. Performs individual file matching only on files with this extension: `.js`.
- **binary**. Performs individual file matching on files with these extensions: `.apklib`, `.bin`, `.dll`, `.exe`, `.o`, and `.so`.
- **all**. Performs individual file matching on all files with these extensions: `.js`, `.apklib`, `.bin`, `.dll`, `.exe`, `.o`, and `.so`.

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

As Docker Compose is no longer supported, the Docker Compose directory has been removed from the distribution and the *Installing Black Duck using Docker Compose* guide is no longer provided.

Embedded license detection

Black Duck can now detect instances of embedded open source licenses not declared by the Black Duck KnowledgeBase for a component.

By enabling detection of deep license data when scanning code, users focused on license compliance can view the licenses that were detected in their open source to ensure there are no problematic licenses and that all licenses are accounted for in their BOM.

With this feature, Black Duck performs a search for license string text and displays the licenses found in the **Source** tab.

Optionally, upload your source files so that BOM reviewers can view discovered license text from within the **Source** tab.

The Signature Scanner has a new parameter **--license-search** to enable searching for embedded licenses. A property to enable deep license data detection will be available in Synopsys Detect version 6.2 and later.

Deep license data added to reports

The component project version report, `components_date_#.csv`, and the component additional fields

report, `bom_component_custom_fields_date_#.csv`, have been enhanced to include deep license data.

The new columns are:

- Deep License Ids
- Deep License Names
- Deep License Families

These fields were added to the end of the `components_date_#.csv` report and prior to the custom fields columns in the `bom_component_custom_fields_date_#.csv` report.

Deep license data has also been added to the Notices File report. This information can be seen in the list of licenses shown for a component as shown in the **Components** section of the report and in the license text shown in the report.

Additional information added to security project version report

The `security_date_time.csv` report has been enhanced and the following fields have been added to the end of the report:

- Overall score
- CWE Ids
- Solution available
- Workaround available
- Exploit available

Improved formatting of copyright reporting in Notices report - Beta

Additional improvements have been made to the formatting of copyright reporting in the Notices report. This feature is *optional* and is currently a Beta feature.

New project version BOM filter

A new filter has been added to the BOM page so that you can view those components that have or do not have comments.

Project version Security tab

The **Published** column has been added to the table shown in the project version **Security** tab.

Consolidated job

To improve job scheduling, a new job, `KbUpdateJob`, replaces the following jobs:

- `KbComponentUpdateJob`
- `KbVersionUpdateJob`
- `KbVulnerabilityUpdateJob`
- `KbVulnerabilityBdsaUpdateJob`

External PostgreSQL database

For users with an external PostgreSQL database, Synopsys recommends upgrading to version 9.6.16 as it includes performance-related fixes. This is the version in the database container.

Also, if your third-party database provider permits it, Synopsys recommends that external PostgreSQL users tune their database by running the following commands:

```
alter system set autovacuum_max_workers = 8 ;
alter system set autovacuum_vacuum_cost_limit = 800 ;
```

and then restart PostgreSQL.

If your third-party database provider does not permit tuning, you do not need to do anything.

Unmapped code locations

Black Duck now provides the capability for you to schedule the cleanup of code locations not mapped to a project version. Configure the `BLACKDUCK_HUB_UNMAPPED_CODE_LOCATION_CLEANUP` and `BLACKDUCK_HUB_UNMAPPED_CODE_LOCATION_RETENTION_DAYS` properties in the `blackduckconfig.env` file.

API Enhancements

- A new matched components endpoint:

`/api/projects/{projectId}/versions/{projectVersionId}/matched-components`

- The following endpoint now returns a `matchConfidencePercentage`:

`/projects/{projectId}/versions/{projectVersionId}/matched-files`

- New vulnerability reports endpoint to show status of all created vulnerability reports:

`/api/vulnerability-reports`

- The following endpoints are intended as a replacement for the existing remediation guidance feature:

`/api/components/{componentId}/versions/{componentVersionId}/upgrade-guidance`

`/api/components/{componentId}/versions/{componentVersionId}/origins/{originId}/upgrade-guidance`

- Added ignored field to the vulnerable BOM components endpoint, which enables filtering based on ignored and unignored components:

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

Supported browser versions

- Safari Version 13.0.4 (14608.4.9.1.4)
- Chrome Version 80.0.3987.100 (Official Build) (64-bit)
- Firefox Version 72.0.2 (64-bit)
- Internet Explorer 11.657.18362.0
- Microsoft Edge 44.18362.449.0
- Microsoft EdgeHTML 18.18363

Container versions

- blackducksoftware/blackduck-postgres:1.0.11
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.6
- blackducksoftware/blackduck-zookeeper:1.0.3
- blackducksoftware/blackduck-nginx:1.0.17
- blackducksoftware/blackduck-upload-cache:1.0.12
- blackducksoftware/blackduck-authentication:2020.2.0
- blackducksoftware/blackduck-webapp:2020.2.0
- blackducksoftware/blackduck-scan:2020.2.0
- blackducksoftware/blackduck-jobrunner:2020.2.0
- blackducksoftware/blackduck-registration:2020.2.0
- blackducksoftware/blackduck-documentation:2020.2.0
- sigsynopsys/appcheck-worker:2019.12
- blackducksoftware/rabbitmq:1.0.3

Japanese Language

The 2019.12.0 version of the UI, online help, and release notes has been localized to Japanese.

Fixed Issues in 2020.2.0

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

- (Hub-20742). Optimized the queries for retrieving data for the Affected Projects page.
- (Hub-20821). Fixed an issue whereby an error message stating that the Black Duck search service was unavailable appeared when adding a component or project.
- (Hub-21833). Fixed a filter issue whereby a user could view components of all projects, instead of just their projects.
- (Hub-22181). Fixed an issue whereby component name and version links were missing on the **Source** tab.
- (Hub-22267). Fixed an issue where the **Created By** column was empty in vulnerability reports.
- (Hub-22310). Fixed an issue whereby the base score for a vulnerability was different in the UI versus in an exported report.
- (Hub-22335). Fixed an issue whereby custom fields were not visible unless the user had the global project viewer role.
- (Hub-22380). Fixed an issue whereby after cloning a project version, notifications for policy violations were still triggered although the policy had been overridden.
- (Hub-22466). Fixed an issue whereby inactive users were not hidden when selecting project owners.
- (Hub-22510). Fixed an issue whereby custom components could not be found when adding or editing a component.
- (Hub-22615). Fixed an issue whereby the KBReleaseupdatejob kept failing.
- (Hub-22626). Fixed an issue whereby scans remained in the post-scan phase but results were uploaded

successfully to Black Duck.

- (Hub-22677). Fixed an issue whereby a component could not be unignored.
- (Hub-22681). Fixed an issue whereby adding a subproject that contained snippets skewed the subproject's component count.
- (Hub-22709). Fixed an issue whereby only 10 values were shown for the dropdown project custom field when creating a policy.
- (Hub-22805). Fixed an issue whereby the `source_date_time.csv` report was empty.
- (Hub-22811). Fixed an issue whereby "role "blackduck_user" does not exist" was seen when attempting to install Black Duck with an external database.
- (Hub-22850). Fixed an issue whereby the `license_term_fulfillment_date_time.csv` report was empty.

Version 2019.12.1

New and Changed Features in Version 2019.12.1

SSO security enhancement

Black Duck has improved the security of the communication between Black Duck and Single Sign-On (SSO) providers. Black Duck now requires that you provide an assertion signature as part the signed response when you configure your SSO Identity Provider (IdP). Although Synopsys does not recommend it, if your IdP is unable to provide this signature, you can disable this added security. Refer to the installation guide for more information.

API enhancement

- New API to update the remediation status of a vulnerability. BOM Component Version vulnerability remediation enables users to read or update the vulnerability remediation status and to add a comment.

Components added without an origin can be accessed with:

```
https://.../api/projects/{projectId}/versions/{versionId}/components/{componentId}/versions/{componentVersionId}/vulnerabilities/{vulnerabilityId}/remediation
```

Components added with an origin can be accessed with:

```
https://.../api/projects/{projectId}/versions/{versionId}/components/{componentId}/versions/{componentVersionId}/origins/{originId}/vulnerabilities/{vulnerabilityId}/remediation
```

Container information

The 2019.12.0 release notes listed the incorrect version of the `blackducksoftware/blackduck-upload-cache` container. The correct version is `blackducksoftware/blackduck-upload-cache:1.0.12`.

Fixed Issues in 2019.12.1

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

- (Hub-21861). Fixed an issue whereby code locations were "broken" after upgrading.
- (Hub-22091). Fixed an issue whereby scanning failed in the `scan.cli` after upgrading to version

2019.12.0.

- (Hub-22737, 22851). Fixed an issue whereby a job failed with an error message indicating there were too many parameters.
- (Hub-22781). Fixed an issue whereby the Edit Component dialog box did not load component or license information.








Version 2019.12.0

New and Changed Features in Version 2019.12.0

Enhancements to the Black Duck UI

The overall navigation of the Black Duck UI has been improved in this release. Enhancements include:

- A new fixed navigation system appears in the left-hand section of the page. Menu options are:

-  **Dashboard**. Displays the last dashboard you viewed.
-  **Find**. A new menu option to view the most recent search results.
-  **Scans**. Displays the Scans page.
-  **Reports**. Displays the Reports page.
-  **Manage**. A new menu option from which you can select: Component Management, Custom Fields Management, License Management, or Policy Management.
-  **Admin**. Displays the Administration page. Note that managing custom field is now available using the  **Manage** option.

- A new Help menu, located on the top navigation bar, provides easy access to the Black Duck online help, integrations help, and API documentation.
- Managing user access tokens has been moved from the My Profile page to a separate page available from the user menu located on the top navigation bar.
- The Tools page has been updated.
- A new filter option, Match Ignore, has been added to the BOM page.

Redesign of project version Security tab

The project version **Security** tab has been redesigned with a new layout, new filters, and new columns added to the vulnerabilities table.

You can now quickly see the CWE ID and whether an exploit, workaround, or solution is available for a

vulnerability without having to drill down to view this information.

Deep level license data

Black Duck now provides the ability to manage your deep licenses (also known as sub-licenses or embedded licenses) which may exist in your open source components. Managing this deep license data reduces the risk of license infringement and makes it easier to understand and report on deep licenses and their risks in the open source being used.

Deep license data is not enabled by default; you must enable including deep license data to your BOM components. Once enabled, any deep licenses, as determined by the Black Duck KnowledgeBase, are automatically active.

Note: Depending upon the number of components and number of deep licenses, enabling the viewing of deep license data can impact the BOM calculation scan time. Adding deep license data to your BOM can affect your license risk and can trigger policy violations.

Copyright data included in Notices report – BETA

An option to include the deduplicated copyright statements obtained from the Black Duck KnowledgeBase to the Notices report is now available. This makes it easy for you to include the full list of copyright holders for the open source components you use in your notice reports.

This feature is *optional* and is currently a Beta feature and results may include poorly formatted or missing copyrights. A known issue is the truncation of copyright statements which contain special characters. Synopsys plans to add additional capabilities around copyright discovery and reporting in future releases.

Please send any feedback on errors or improvements to your Synopsys representative or to our customer support organization.

Custom license family enhancements

- To eliminate confusion, the Restricted Third Party Proprietary license family has been renamed to Restrictive Third Party Proprietary.
- KnowledgeBase licenses are now associated with the Restrictive Third Party Proprietary license family. This may affect your license risk and can trigger policy violations.

Policy management enhancement

Policy management now provides the ability to create policy rules based on these vulnerability conditions:

- CWE IDs
- Exploit Available
- Overall Score
- Solution Available
- Workaround Available

Enhancements to the report database

New views have been added to the `reporting` schema of `bds_hub` for project, project version, and BOM component custom fields.

BOM status

The header in the project version BOM page (also known as the project version **Components** tab) now includes the status of components, indicating whether processing is occurring to update the BOM.

Custom Scan Signatures

The Custom Scan Signatures feature is now available to all customers.

Custom Fields enhancements

Black Duck now provides the ability to delete custom fields.

API enhancements

- Custom fields are prevented from being deleted if they are in use in a policy.

The DELETE endpoint for custom fields returns an error if the custom field is being used in a policy.

Support for non-root user ID/Group IDs

This release adds support for running Black Duck images using non-root user IDs/Group IDs in `.yaml` configuration files for Kubernetes.

Supported browser versions

- Safari Version 13.0.3 (14608.3.10.10.1)
- Chrome Version 78.0.3904.108 (Official Build) (64-bit)
- Firefox Version 71.0 (64-bit)
- Internet Explorer 11.476.18362.0
- Microsoft Edge 44.18362.449.0
- Microsoft EdgeHTML 18.18363

Container changes

- blackducksoftware/blackduck-postgres:1.0.10
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.5
- blackducksoftware/blackduck-zookeeper:1.0.3
- blackducksoftware/blackduck-nginx:1.0.14
- blackducksoftware/blackduck-upload-cache:1.0.11
- sigsynopsys/appcheck-worker:2019.12
- blackducksoftware/rabbitmq:1.0.2

Renamed job

The `KbReleaseUpdateJob` has been renamed to the `KbVersionUpdateJob` to better describe the purpose of the job.

New audit event

An audit event will now appear when the Black Duck KnowledgeBase deprecates a component or component

version.

Japanese language

The 2019.10.0 version of the UI, online help, and release notes has been localized to Japanese.

Fixed Issues in 2019.12.0

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

- (Hub-13468). Fixed an issue whereby the Used Count value shown in the Black Duck UI was incorrect.
- (Hub-16211, 16713, 17562). Fixed an issue whereby the BOM appeared up-to-date, however, processing was still occurring.
- (Hub-16950). Removed external images from the webapp container.
- HUB-17685). Fixed an issue whereby the policy violation status was not updated after the policy violation for reviewed components no longer occurred.
- (Hub-17841). Fixed an issue whereby the `scans.csv` project version report displayed the code location ID in the Scan ID field.
- (Hub-18257). Removed gravatar from Black Duck.
- (Hub-18978). Fixed an issue whereby a component could not be deleted from a project version.
- (Hub-20997, 21968). Fixed an issue whereby not all matched components were listed on the Scans > Components page.
- (Hub-21205). Fixed an issue whereby an input parsing request error was received when attempting to view match results on the **Source** tab.
- (Hub-21319). Fixed an issue whereby the scan history showed matches, however, the Scans > Components page showed no results.
- (Hub-21353). Fixed an issue whereby the license for a component version could not be modified.
- (Hub-21369). Fixed an issue whereby filtering a component search by primary language did not work correctly.
- (Hub-21538). Fixed an issue whereby the Snippet View window on the **Source** tab did not appear when using Edge and IE 11 browsers.
- (Hub-21606). Fixed an issue whereby the "New projects created this week" filter returned all projects.
- (Hub-21614). Fixed an issue whereby side-by-side matched code was not highlighted in the Snippet View window on the **Source** tab.
- (Hub-21664). Fixed an issue whereby the corresponding matched lines in the source code pane did not change when the alternative match was selected on the **Source** tab.
- (Hub-21735). Fixed an issue whereby a "createOrUpdateMany.arg1.compositePath required" error appeared when trying to update a blank dependency's component on the **Source** tab.
- (Hub-21751). Revised the text on the SAML logout page.
- (Hub-21785). Fixed an issue whereby the filter on the **Source** tab did not display all existing files and/or directories.
- (Hub-21793). Fixed an issue whereby the Black Duck 2019.8.0 AMI was missing images.
- (Hub-21796). Fixed an issue whereby changes to a file or directory match made to a child directory propagated to the parent directory on the **Source** tab.

- (Hub-21817). Fixed an issue whereby icons were missing on the Tools page.
- (Hub-21960). Fixed an issue whereby the VersionBomComputationJob was failing with the following error message: duplicate key value violates unique constraint "uidx_vuln_remediation_release_vuln_id".
- (Hub-22042). Fixed an issue whereby links to deprecated integrations were still shown on the Tools page.
- (Hub-22090). Fixed an issue whereby updating the status for a component version on the component version **Settings** tab was unsuccessful.
- (Hub-22094, 22477). Fixed an issue whereby LDAP authentication was unsuccessful after upgrading to version 2019.10.0.
- (Hub-22165). Fixed an issue whereby the API endpoint GET /api/vulnerabilities/{vulnerabilityId}/affected-projects was missing access controls.
- (Hub-22167). Fixed an issue whereby selecting an empty license from the License Management table displayed a 404 error.
- (Hub-22175). Fixed an issue whereby the file path no longer appeared when hovering over a matched file on the **Source** tab.

Version 2019.10.3

New and Changed Features in Version 2019.10.3

Black Duck version 2019.10.3 is a maintenance release and contains no new or changed features.

Fixed Issues in 2019.10.3

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

- (Hub-22803). Fixed a potential issue in the Black Duck SSO integration by providing greater security when communicating between Black Duck and the SSO provider.

Version 2019.10.2

New and Changed Features in Version 2019.10.2

Black Duck version 2019.10.2 is a maintenance release and contains no new or changed features.

Fixed Issues in 2019.10.2

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

- (Hub-22091). Fixed an issue whereby scanning failed in the `scan.cli` after upgrading to version 2019.10.0.

Version 2019.10.1

New and Changed Features in Version 2019.10.1

Black Duck version 2019.10.1 is a maintenance release and contains no new or changed features.

Fixed Issues in 2019.10.1

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

- (Hub-21912). Fixed an issue whereby the Documentation and Webapp containers would not start when using Docker Swarm with a read-only deployment.
- (Hub-21965). Fixed an issue whereby Black Duck did not work with proxy certificate settings.
- (Hub-21970). Fixed an issue whereby the **Legal** tab was only visible to License Managers.
- (Hub-22002). Fixed an issue whereby the `blackduck_reporter` user did not have permission to access data using the `reporting` schema in `bds_hub`.
- (Hub-22056). Fixed an issue whereby a project version report was failing with a validation exception.

Version 2019.10.0

New and Changed Features in Version 2019.10.0

Redesigned report database

To make it easier for you to quickly create, use, back up, and restore your reporting database, as of the 2019.10.0 release, the tables from the separate reporting database (`bd_hub_report`) have been moved from the `public` schema in the reporting database to the `reporting` schema in the Black Duck database, `bds_hub`.

Tables in the reporting schema in the Black Duck database are:

- Component
- Component license
- Component match type
- Component matches
- Component policies
- Component usage
- Component vulnerabilities
- Project
- Project mapping
- Project version
- Project version code locations

There will be a delay for any changes made in Black Duck to appear in the report database. The length of time for this delay depends on the value you specified using the new `BLACKDUCK_REPORTING_DELAY_MINUTES` environment variable, which by default, equals 8 hours. Refer to the installation guide for more information.

While Black Duck provides the `blackduck_reporter` user which only has read-only access to the reporting schemas of the `bds_hub` database, you can configure additional users which have the same permissions as the `blackduck_reporter`. Refer to the *Report Database* guide for more information.

Note: Synopsys recommends that VulnDB users or former VulnDB users back up the `bds_hub_report` database. For all other users, data that was in the `bds_hub_report` database is now in the `bds_hub` database. For more information, refer to the installation guide.

Enhancements to user management for LDAP/SSO

You can now create a Black Duck user account for a local user (an internal user account) or for an external user (such as a user managed by an external source, such as LDAP).

Note that with external user accounts:

- You can create users and assign roles without the user logging in to Black Duck.
- User information, such as the first or last name, can be changed in Black Duck, however passwords are not managed by Black Duck.
- The first name, last name, and email address of the external user will be overridden with the information present on the external server, (such as an LDAP server), at the time of login.

Note: Any user accounts created before the 2019.10.0 release are internal users.

Enhancement to group management

Black Duck now provides the ability for you to create one or more default groups. Subsequent new users are automatically added to this group and are granted all roles and access to all projects configured for this group.

Black Duck UI enhancement for critical and high security risks

The critical and high security risk values are now shown in separate categories in the Black Duck UI.

Note: If you selected to view CVSS 2.0, the graphs display the Critical risk category with a value of 0.

Ability to specify number of scanning levels for Custom Scan Signature, now a Limited Customer Availability feature.

Custom scan signatures by default, are limited to the top five levels in the directory structure. In this release, system administrators can now modify this global default value and Super Users or Project Managers can modify the setting for a specific project.

Note that this feature is now a “Limited Customer Availability” offering which is available to specific Black Duck customers. Though the custom scan signature feature is fully functional with full product support, Synopsys is limiting production use to a subset of customers who participated in the Beta program. As such, the feature is expected (but not guaranteed) to perform at production level workloads and customers may need to adjust their use of the feature to address their particular environments and workloads. If you did not participate in the Beta program and would like to test this capability in a non-production environment, please reach out to your product representative to have the feature enabled.

Additional status values for license and component management

The following statuses have been added to License Management:

- In Review
- Reviewed
- Deprecated

The following statuses have been added to Component Management:

- In Review
- Reviewed

With these additions, the possible status values for license and component management are:

- Unreviewed
- In Review
- Reviewed
- Approved
- Limited Approval
- Rejected
- Deprecated

Note that the unreviewed status is not available when adding a KnowledgeBase component.

Additional license families

Two new license families – Restricted Third Party Proprietary and Internal Proprietary – have been added to Black Duck. Note that in this release of Black Duck, there are no KnowledgeBase licenses associated to these new license families.

Note: If your License Manager created a custom license family labeled "Restricted Third Party Proprietary" or "Internal Proprietary" before the 2019.10.0 release, the number "(1)" is appended to those custom license family names.

Refer to the documentation to view the risk associated with these license families.

Enhancements to the component and component additional fields project version reports

The component project version report, `components_date_#.csv`, and the component additional fields report, `bom_component_custom_fields_date_#.csv`, have been enhanced to include more information. These columns have been added::

- File Match Count
- License Risk
- Component Status
- Component Notes
- Fulfillment Required
- Version Notes
- Critical Vulnerability Count
- High Vulnerability Count
- Medium Vulnerability Count
- Low Vulnerability Count
- Release Date
- Newer Versions

- Commit Activity
- Commits in Past 12 Months
- Contributors in Past 12 Months

These fields were added to the end of the component project version report. For the component additional fields report, these fields appear before the BOM component, component, and component version custom field information.

New API documentation and enhancements

New API documentation is now available. This documentation makes APIs easier to use by grouping APIs, providing improved examples, and adding API linking. This documentation is located at:

<https://<Black Duck Server URL>/api-doc/public.html>

The previous version of the API documentation is still available. To view it, go to <https://<Black Duck Server>/api.html>

Other API enhancements consist of:

- Added PUT support for ignored flag, inAttributionReport and attributionStatement to BOM component API.
- Added public API to update license text in the BOM license modal ([api/projects/id/versions/id/components/id/versions/id/licenses/id/text](#)).
- Added new public APIs for interacting with Jobs at [/api/jobs](#) and [/api/jobs/{jobId}](#).
- Updated the [/api/user](#) API to enable adding/editing the externalUserName and type fields.

Ability to configure the user session timeout value

Black Duck now provides the ability for you to configure a user session timeout value that automatically log out users from the Black Duck server.

To change the current timeout value, make the following PUT request with the PUT request body.

```
PUT https://<hub-server>/api/system-oauth-client
{
  "accessTokenValiditySeconds": <time in seconds>
}
```

Refer to the installation guide for more information.

Removal of the bdio database

To improve scan upload performance from the client to Black Duck, the `bdio` database is no longer used and will be removed in a future release. As a result, the `ScanGraphJob` has also been removed.

You can back up the `bdio` database and/or truncate all table data if you want to reclaim space.

Supported browser versions

- Safari Version 13.0.1 (14608.2.11.1.11)
- Chrome Version 77.0.3865.90 (Official Build) (64-bit)
- Firefox Version 69.0.2 (64-bit)

- Internet Explorer 11.1006.17134.0
- Microsoft Edge 42.17134.1.0
- Microsoft EdgeHTML 17.17134

Container changes

Updated containers:

- uploadcache: image: blackducksoftware/appcheck-worker:2019.09
- webserver: image: blackducksoftware/blackduck-nginx:1.0.9

Changed namespace:

- binaryscanner: image: sigsynopsys/appcheck-worker:2019.09

Japanese Language

The 2019.8.0 version of the UI, online help, and release notes has been localized to Japanese.

Fixed Issues in 2019.10.0

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

- (Hub-19787). Fixed an issue whereby four simultaneous VersionBomComputationJobs started for a single project version and all of these jobs failed.
- (Hub-20000). Fixed an issue whereby the full file path information was not shown in the snippet view on the **Source** tab.
- (Hub-20040). Fixed an issue whereby the logout page did not appear when logging out of an SSO account.
- (Hub-20366). Fixed an issue so that users would not get a timeout when attempting to upload a `.json` file when using the Black Duck UI.
- (Hub-20421). Fixed an issue so that the Black Duck UI does not display upgrade guidance information when a upgrade version is not available.
- (Hub-20770). Fixed an issue whereby the snippet view on the **Source** tab did not show the file name of the matching component.
- (Hub-20879). Fixed an issue whereby the **Source** tab did not display the full path if a file or folder was located within an archive file.
- (Hub-19534, HUB-20800, HUB-20926). Fixed an issue whereby the KbReleaseUpdateJob failed repeatedly which also caused duplicate components to appear on the Component Dashboard.
- (Hub-21075). Fixed an issue whereby scans were mapped to the incorrect project versions and deleted project versions were restored.
- (Hub-21217). Fixed an issue whereby cloning a project failed with a "server did not respond in time" error message.
- (Hub-21264). Fixed an issue with an invalid port when integrating SSO with Black Duck.
- (Hub-21276). Fixed an issue whereby an AGPL license violation did not clear after the policy violation was overridden.
- (Hub-21298, HUB-21549). Fixed an issue whereby editing ignored components in a BOM resulted in a 404 error.

- (Hub-21421). Fixed an issue whereby printing the BOM failed for large projects.
- (Hub-21464). Fixed an issue whereby the User Management page displayed a maximum of 10 groups per user.
- (Hub-21488). Fixed an issue whereby external users were being removed from groups at login with Azure AFDS SAML.
- (Hub-21538). Fixed an issue whereby snippet alternative matches were broken when viewed in Edge 11 and Internet Explorer 11.
- (Hub-21541). Fixed an issue whereby the authentication container was returning an incorrect port when running Kubernetes on AWS.

Version 2019.8.1

New and Changed Features in Version 2019.8.1

API Enhancements

- The API endpoints for ignoring, confirming, or editing snippet matches are now available.
- Provided the ability to retrieve file match checksum data for a Protex BOM import so that it can be compared against checksum file match data from a Black Duck scan.

Fixed Issues in 2019.8.1

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

- (HUB-20587). Fixed an issue whereby the **Source** tab allowed users to add a project to itself when editing a component.
- (Hub-21057). Fixed performance issues seen after upgrading to version 2019.6.1.
- (Hub-21372). Fixed an issue whereby notification_subscriber state updates were very slow.

Version 2019.8.0

New and Changed Features in Version 2019.8.0

Security enhancements

- The Black Duck UI now displays an overall score for a vulnerability and its associated risk level. The Security Dashboard, the *Component Name Version Security* tab, and the Black Duck KB *Component Name Version Security* tab now have an **Overall Score** column which shows the Temporal score (for BDSA), or Base score (for NVD). Hover over the **Overall Score** value to see the individual values.
 - For BDSA, the Temporal, Base, Exploitability, and Impact scores are shown.
 - For NVD, the Base, Exploitability, and Impact scores are shown.

To help you quickly find vulnerabilities that interest you, a new filter "Overall Score greater than or equal to X" has been added to the *Component Name Version Security* tab.

- A new policy condition, Highest Vulnerability Score, also has been added so that you can create policy rules based on the vulnerability score to help you identify your most critical vulnerabilities.

Additional component usages

In this release, Black Duck has added the following usages:

- **Merely aggregated.** Your project does not use the component; it may be on the same media, but is not related. The components exist together, but do not depend upon each other in any way. For example, including a sample version of an unrelated product with your distribution.
- **Prerequisite.** This usage is for components that are required but not provided by your distribution.

Enhancements to component management

To make it easier to manage component versions in Component Management, there is a new **Component Versions** tab.

Enhancements to audit information

Project and project version audit information has been enhanced to now include information regarding the original license (when the original license is modified), rescans, and fulfillment of license terms.

Cloning enhancements

Cloning has been enhanced so that the **Component Edits** option now includes cloning of confirmed snippet adjustments and policy violation overrides and associated comments.

Improved security for storage of user credentials

User credentials are now stored in the Black Duck database using random-salt SHA256.

Component custom fields project version report

The Project Version report has been enhanced to include a new option: **Component Additional Fields**. Selecting this option produces a new report, `bom_component_custom_fields_date_#.csv`, which includes the same information as the `component_date_#.csv` report but also includes BOM component, component, and component version custom field labels and values for this project version.

The option for the project version custom fields `.csv` report has been renamed to **Project Version Additional Fields**.

Snippet scanning enhancements

In order to improve scanning performance and results, when customers select to perform snippet scans, the snippet scans will first check unmatched file candidates for a file level match, prior to checking the file contents for snippets. If a file level match is detected, potential candidates are generated from that result set. If no file level matches are detected, then normal snippet scanning over the file contents is conducted. For customers highly dependent upon the snippet matching capability and who use lots of unmodified OSS files, this can lead to significant scan performance improvements as well as better match results. In addition, customers will be able to view/filter on files which are exact matches to OSS to aid in confirmation/review process.

Supported Docker Versions

Black Duck installation supports Docker versions 18.03.x, 18.06.x, 18.09.x, and 19.03.x (CE or EE).

Upgraded BDBA container

The updated Black Duck Binary Analysis container (now version 2019.06) includes these features and bug fixes:

Features:

- Extract package information from distro package files, supports .deb, .rpm, .apk, .pkg.
- Added support for extracting UEFI firmware images.
- Upgraded libmagic to 5.37 - improves file type identification and fixes CVE-2019-8907.
- Added improved support for detecting Go components from Windows and MacOS binaries.
- Added detection of many popular components in uClinux.
- Added support for extracting InstallShield 2016 and older generated Windows installers.

Bug fixes:

- Fixed regression with lzma-compressed ulimages that were corrupted.
- Fixed regression when extracting VMware's version of tar.
- Fixed slow JWT token extractor in some corner cases.
- Changed from using "command" to using "entrypoint" in the docker-entrypoint.sh file due to internal start up script changes.

Updated containers

- uploadcache: image: blackducksoftware/blackduck-upload-cache:1.0.9
- webserver: image: blackducksoftware/blackduck-nginx:1.0.8

API enhancements

New endpoint to find affected projects by vulnerability:

- GET /api/vulnerabilities/{vulnerabilityId}/affected-projects

New job-related endpoints:

- Get job filters: GET /api/jobs-filters
- Get jobs by job ID: GET /api/jobs/{jobId}
- Delete jobs by job ID: DELETE /api/jobs/{jobId}
- Reschedule jobs by job ID: PUT /api/jobs/{jobId}

Deprecated endpoints:

- GET /api/components/{componentId}/vulnerabilities
- GET /api/projects/{leftProjectId}/versions/{leftVersionId}/compare/projects/{rightProjectId}/versions/{rightVersionId}/components

APIs added to the new BETA API documentation, located at [HTTPS://<Black Duck Server URL>/api-doc/public.html](https://<Black Duck Server URL>/api-doc/public.html):

- Report API Endpoints
- Scan Analysis Upload API Endpoint
- Additional Scan Code Location API Endpoints

Fixed Issues in 2019.8.0

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

- (HUB-18804). Fixed an issue whereby a user with the Global Code Scanner role and the Project Creator role could access any project.
- (HUB-18930). Fixed an issue whereby importing a Protex BOM into Black Duck failed.
- (HUB-19690). Fixed an issue whereby a user with the Project Code Scanner role was unable to view the *Scan Name* page to view assigned project scans or unmap existing scans.
- (HUB-19864). Fixed an issue whereby vulnerability reports consistently failed.
- (HUB-19875). Fixed an issue whereby a snippet scan failed due to "Premature end of chunk coded message body."
- (HUB-20064). Fixed an issue whereby the **Related to** column in the Jobs page was not populated for the SnippetScanAutoBomJob job.
- (HUB-20085). Fixed an issue whereby the snippet scan did not finish.
- (HUB-20101). Fixed an issue whereby the **Source** tab was inconsistent when navigating to match names.
- (HUB-20192). Fixed an issue whereby the **Source** tab incorrectly displayed an unconfirmed status for confirmed and/or matched snippets.
- (HUB-20202, 20236). Fixed an issue whereby the Scan CLI exited a scan with code 70.
- (HUB-20223). Fixed an issue whereby the Protex BOM Tool did not import file match data.
- (HUB-20228). Fixed an issue whereby the side-by-side snippet feature on the **Source** tab did not update the content on the left (source) side.
- (HUB-20244). Fixed an issue whereby the number of components matched as shown on the *Scan Name* page was different than the number of components in the `source.csv` report.
- (HUB-20358). Fixed an issue whereby scanning failed with a "For input string: 0.07" error.
- (HUB-20370). Fixed an issue whereby selecting a match in the **Source** tab did not expand the tree to show the location of the match.
- (HUB-20483). Fixed an issue whereby the match lines did not appear for a snippet match in the **Source** tab.
- (HUB-20587). Fixed an issue whereby the **Source** tab allowed users to add a project to itself when editing a component.
- (HUB-20588). Fixed an issue to allow using main search algorithm for component name modal searches.
- (HUB-20611). Fixed an issue whereby the ScanPurgeJob job logged failures because of a missing or invalid component Black Duck identifier.
- (HUB-20688). Fixed an issue whereby a different component version could not be selected in the Edit Component dialog box.
- (HUB-20733). Fixed an issue whereby "The application has encountered an unknown error" message appeared when attempting to import a Protex BOM into Black Duck.
- (HUB-20744). Fixed an issue whereby attempts to edit 100 snippet matches timed out.

- (HUB-20749). Fixed an issue whereby a user with the Project Code Scanner role could not upload source files.
- (HUB-20755). Fixed an issue whereby unconfirmed or ignored snippets appeared in the project version cryptography report.
- (HUB-20794). Removed the `invisible.vbs` file from the `scan.cli-windows-version.zip` file.
- (HUB-20870). Fixed the API call that provides the project ID from a passed application ID.
- (HUB-20886, 20918). Fixed an issue whereby a user's read/view permissions for viewing or accessing a project were not enforced.
- (HUB-20969). Fixed an issue whereby vulnerability remediation information entered by the user was not updated in the Black Duck UI.

Version 2019.6.2

New and Changed Features in Version 2019.6.2

Black Duck version 2019.6.2 is a maintenance release and contains no new or changed features.

Fixed Issues in 2019.6.2

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

- (HUB-19716). Fixed an issue whereby the following error message was seen: "The column index is out of range: 8, number of columns: 7".
- (HUB-20899). Fixed an issue whereby the `KBReleaseUpdateJob` continually failed.

Version 2019.6.1

New and Changed Features in Version 2019.6.1

Removal of the `kubernetes` directory and files

The `kubernetes` directory and all files located in that directory have been removed.

Synopsys recommends installing Black Duck on Kubernetes or OpenShift using Synopsys Operator.

- Click [here](#) for an overview of Black Duck for Kubernetes/OpenShift.
- Click [here](#) for an overview of Synopsys Operator.
- Click [here](#) for documentation on installing Black Duck by using Synopsys Operator.

Fixed Issues in 2019.6.1

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

- (HUB-19013). Fixed an issue whereby the `VersionBomComputationJob` failed after a project or project version was deleted.
- (HUB-20223). Fixed an issue whereby the Protex BOM tool (`scan.protex.cli.sh`) did not import file match data.
- (HUB-20463). Fixed an issue whereby the file tree shown in the left pane of the **Source** tab did not load on

a hosted server.

- (HUB-20484). Fixed an issue whereby some components in a project could not be reviewed or ignored.
- (HUB-20494). Fixed an issue whereby a transitive dependency was reported as a direct dependency.
- (HUB-20540). Fixed an issue whereby the KBReleaseUpdateJob failed with an error message stating "findSnippetAdjustment.arg3 can't be blank."
- (HUB-20612). Fixed an issue whereby users with the Project Manager or Project Code Scanner role could not view and/or unmap scans using the *Project Version* **Settings** tab.

Version 2019.6.0

New and Changed Features in Version 2019.6.0

Common Vulnerability Scoring System (CVSS) 3.0 security risk scores

Black Duck now provides you with the option of viewing CVSS 3.0 scores. Users with the system administrator role can redefine the order of security ranking that Black Duck uses to define the risk score and risk categories of security vulnerabilities. By default, Black Duck displays CVSS 2.0 scores.

Note that changing the order of the security risk configuration will result in revised security risk calculations for all project version BOMs and may result in new policy violations. These calculations may take a *considerable amount of time* to complete

When changing the security ranking, these two new jobs are started:

- VulnerabilityReprioritizationJob, which recomputes all BOMs with the new vulnerability priority setting.
- VulnerabilitySummaryFetchJob, which locates missing CVSS 3.0 data.

License term fulfillment

License Managers can now define which license terms require fulfillment. The fulfillment status of a license term is defined for a term at the license level, as not all instances of a license term may require fulfillment. This allows you to easily define the fulfillment requirements for a license term,

- BOM Manager's use the new *Project Version's* **Legal** tab, enabled by the System Administrator, to view all license terms that require fulfillment and indicate which license terms are fulfilled.
- Policy managers can create a policy rule that will trigger a violation when there are unfulfilled license terms.
- License term fulfillment status can be cloned.
- A new project version report, `license_term_fulfillment.csv` lists the license terms and fulfillment status for a project version.
- A new job, LicenseTermFulfillmentJob, applies license term fulfillment requirements to all BOMs.

Enhancements to custom fields

Black Duck now supports the creation and management of custom fields for BOM components and component versions.

BOM component custom field information appears when viewing the details of a component in the BOM.

Component version custom field information is shown in the **Additional Fields** section of the *Component Name*

Version Name **Settings** tab.

Enhancements to reports

The following enhancements have been made to reports:

- Project version reports:

- The following characters < > \ / | : * ? + " in the project or version name are replaced with underscores (_).
- The archive filename is <ProjectName-ProjectVersion>_YYYY-MM-DD-HHMMSS.zip (time stamp in UTC).
- The directory and filename are <ProjectName-ProjectVersion>_YYYY-MM-DD-HHMMSS/<fileName>_YYYY-MM-DD-HHMMSS.csv (with the same time stamp as the archive filename)

- Global vulnerability reports:

- The Vulnerability Remediation report, Vulnerability Status report, and the Vulnerability Update report now have a `.csv` option for the format of the report.

This option is useful if your data set becomes too large to render and view in the browser.

- The archive file name is now vulnerability-<ReportType>-report_YYYY-MM-DD-HHMMSS.zip (time stamp in UTC).
- Directory and filename are: vulnerability-<ReportType>-report_YYYY-MM-DD-HHMMSS.csv (with the same time stamps as the archive filename)
- These new columns have been added to all global vulnerability reports:
 - Remediation updated at
 - Security Risk

These new columns are now the last two columns in the reports.

New API documentation - BETA

New API documentation is now available. This documentation makes APIs easier to use by grouping APIs, providing improved examples, and adding API linking.

This documentation is located at:

[HTTPS://<Black Duck Server URL>/api-doc/public.html](https://<Black Duck Server URL>/api-doc/public.html)

Note that this documentation is a Beta feature and all APIs may not yet be represented.

The existing API documentation, located at [HTTPS://<Black Duck Server URL>/api.html](https://<Black Duck Server URL>/api.html) is still available.

Improvements to the Source view

The Source view has been enhanced and now includes the ability to copy a path to the clipboard and the ability to bulk edit components tied to snippet.

Support for read-only file system for Swarm Services

A new file, `docker-compose.readonly.yml`, is included in the distribution. Use this file to install Black

Duck with a read-only file system for Swarm services.

This feature is supported for Docker Swarm only.

Docker Swarm orchestration version changes

- Docker compose version: 3.6
- Docker engine version: 18.02.0+

Enhancement to archived project versions

For project versions in the Archived phase, updates from the Black Duck KnowledgeBase regarding security vulnerabilities are applied to archived project versions.

However, all other updates from the Black Duck KB, such as updates to license information, *are not* applied to archived project versions.

New jobs

These jobs have been added to Black Duck:

- BomAggregatePurgeOrphansJob, which deletes any BOM data not associated with a project version.
- ComponentDashboardRefreshJob, which refreshes the information shown on the component dashboard.
- PolicyRuleModificationBomComputationJob, which computes version BOMs affected by changes to policy rules.

Enforcement of code size limit

If you exceed your code size limit, an error message now appears when trying to scan (for example, shown in log files in Jenkins or on the screen in Synopsys Detect (Desktop)) or when uploading scans to Black Duck. You will not be able to scan or upload scans if you exceed your code size limit.

Updated Black Duck - Binary Analysis container

The updated Black Duck Binary Analysis container (now version 2019.03) includes:

- Added detection for new components
- Added support for extracting Linux packages created with InstallAnywhere
- Added support for extracting zstandard compression
- Added support for FreeBSD ufs, uzip and ulzma image extraction

Enhancements to Synopsys Detect (Desktop)

Synopsys Detect (Desktop), formerly known as Black Duck Detect Desktop, now includes these features:

- Ability to use an existing API key.
- An option to migrate your data from a previous version of Synopsys Detect (Desktop).
- Ability to check for updates of Synopsys Detect (Desktop) to see if newer versions are available. This option is only available for Windows and MacOS systems.

As the application installs into a directory related to its name, Synopsys Detect (Desktop) will not uninstall previous versions of Black Duck Detect Desktop. It also will not uninstall versions of Synopsys Detect

(Desktop) that were installed in a non-default directory. You must manually uninstall all previous versions of Black Duck Detect Desktop, versions of Synopsys Detect (Desktop) installed in the non-default directory, and fix or delete any shortcuts.

Removal of Solr container

For improved search performance, the Solr container has been removed.

Depending upon your individual corporate policy, you can keep, back up, or remove the existing Docker Solr volume,

Component Dashboard refresh rate

By default, the Component Dashboard refreshes every 5 minutes. If you notice a lag between your changes and the information appearing on the Component Dashboard, you can now add a system property, `com.blackducksoftware.bom.aggregate.component_dashboard_refresh_interval_ms`, to the `blackduck-config.env` file that defines the Component Dashboard refresh rate.

This feature is for Docker Compose and Docker Swarm.

Japanese Language

The 2019.4.1 version of the UI, online help, and release notes has been localized to Japanese.

Fixed Issues in 2019.6.0

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

- (HUB-8192). Notifications older than 180 days are now automatically deleted.
- (HUB-13279). The complex license view model is now included in the project version APIs in the new Beta API documentation.
- (HUB-15298). Fixed an issue whereby performance issues occurred when accessing the **Component** tab.
- (HUB-15698). Fixed an issue whereby policy violations were not shown for snippets on the **Source** tab.
- (HUB-16619). Fixed an issue whereby unconfirmed snippets triggered vulnerability notifications and were included in security risk values.
- (HUB-16628). Fixed an issue whereby navigating to a direct Black Duck link when SSO was enabled brought you to the Project dashboard after logging in, instead of the original link destination.
- (HUB-17378). Fixed an issue whereby snippet scans were double counted against the total code size limit.
- (HUB-18221). Fixed an issue whereby a user with the Global Code Scanner and Project Creator roles could view the Scans page or a *Scan Name* page and access a project version which they did not have permission to view.
- (HUB-18523). Fixed an issue whereby users with the Project Code Scanners role could not download scans for the projects to which they are assigned.
- (HUB-18561). Fixed an issue whereby selecting to view a CVE or BDSA record displayed an empty page when using Internet Explorer.
- (HUB-18623). Fixed an issue whereby the Operational Risk filter changed to the License Risk filter when a page was reloaded.
- (HUB-18631). Fixed an issue whereby a 404 error message appeared when adding or editing a comment.

- (HUB-18676). Fixed an issue whereby a 400 error message appeared when analyzing a binary file.
- (HUB-18694). Fixed an issue so that the `system_check.sh` script now uses the container's proxy settings when probing external URLs.
- (HUB-18760). Fixed an issue whereby the cryptography filter worked incorrectly in the BOM page and the match type filter in policy management was missing the Unmatched option.
- (HUB-18911). Renamed the Attribution Report filter on the BOM page to Notices File Report.
- (HUB-18983). Fixed an issue whereby an SSO user who did not have project-level permissions but did have full global permissions received an error when policy checking was enabled when scanning with Synopsys Detect.
- (HUB-19130). Fixed an issue whereby the number of components matched as shown on the *Scan Name* page was different than the number of components in the `source.csv` report.
- (HUB-19141). Fixed an issue so that only confirmed snipped components appear on the Component Dashboard.
- (HUB-19238). Fixed a issue where it appeared that edits to the BOM did not complete in a timely manner.
- (HUB-19274). Fixed an issue where inconsistency was seen in the security risk categorization in the Black Duck UI versus the `security.csv` report.
- (HUB-19490). Fixed an issue whereby filters on the BOM page displayed incorrect values when a page was refreshed.
- (HUB-19504). Fixed an issue so that the scan client CLI is now packaged with Java JRE version 11.0.2.
- (HUB-19522). Fixed an issue whereby users with the Project Code Scanner role got an exit code 77 although the scan completed and uploaded to Black Duck.
- (HUB-19548). Fixed an issue whereby manual changes to a license family did not propagate to projects unless the project was rescanned.
- (HUB-19604). Fixed an issue whereby inaccurate search results appeared when attempting to add a subproject.
- (HUB-19607). Fixed an issue whereby the BDSA record for some security vulnerabilities did not display the related CVE record in the **Security** tab.
- (HUB-19637). Fixed an issue whereby unconfirmed or ignored snippet matches were included in the vulnerable BOM components API response.
- (HUB-19696). Fixed an issue so that `/api/components/{componentId}` sublinks to references, custom-fields, origins, risk-profile, and vulnerabilities now redirect correctly.
- (HUB-19728). Fixed an issue whereby "The entity does not exist" error message appeared when attempting to clone a project version.
- (HUB-19771). Fixed an issue whereby the edit section of the **Source** tab did not consistently open when a directory was selected.
- (HUB-19791). Fixed various UI issues in the **Source** tab when managing snippets.
- (HUB-19897). Fixed an issue when a user could not be assigned to more than one project if that user already had access to one of the projects.
- (HUB-19907). Fixed an issue whereby the findVulnerableComponents API incorrectly showed vulnerabilities and notifications for ignored components and unconfirmed snippets in a project.
- (HUB-19909). Fixed an issue whereby an "Unable to manage operation because it is not supported by

policy for job type" message appeared when performing medium to large scans.

- (HUB-20033). Fixed an issue whereby the Jobs page timed out and displayed the "Black Duck Server does not respond" message.
- (HUB-20054). Fixed an issue whereby selecting a different component for a snippet match added the component instead of replacing the existing component.
- (HUB-20086). Fixed an issue whereby a 412 Precondition failed error appeared when using the file license API.
- (HUB-20146). Fixed an issue whereby an "Unable to create component adjustment because it already exists" error message appeared when attempting to clone a project.
- (HUB-20172). Fixed an issue whereby selecting the path did not display the exact path or file name for declared components in the **Source** tab.

Chapter 3: Known Issues and Limitations

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

- When scanning with the Signature Scanner CLI, Synopsys Detect (Desktop), or Synopsys Detect, you may see error messages that starts with the following:

```
ERROR StatusLogger Unrecognized
```

You can ignore these messages. These errors do not impact the scans and will not cause the scan to fail.

- The **Overview** tab for the *Component Name* page shows CVSS 2.0 data, even if you selected to view CVSS 3.0 (NVD or BDSA) data.
- 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.