BLACKDUCK

BY SYNOPSYS®

Release Notes

Version 2021.4.2

This edition of the *Release Notes* refers to version 2021.4.2 of Black Duck.

This document created or updated on Tuesday, June 15, 2021.

Please send your comments and suggestions to:

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

Contents

Black Duck documentation

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

Title	File	Description
Release Notes	release_notes.pdf	Contains information about the new and improved features, resolved issues, and known issues in the current and previous releases.
Installing Black Duck using Docker Swarm	install_swarm.pdf	Contains information about installing and upgrading Black Duck using Docker Swarm.
Getting Started	getting_started.pdf	Provides first-time users with information on using Black Duck.
Scanning Best Practices	scanning_best_practices.pdf	Provides best practices for scanning.
Getting Started with the SDK	getting_started_sdk.pdf	Contains overview information and a sample use case.
Report Database	report_db.pdf	Contains information on using the report database.
User Guide	user_guide.pdf	Contains information on using Black Duck's UI.

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

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

Black Duck integration documentation 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
- Phone: See the Contact Us section at the bottom of our support page to find your local phone number.

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

Another convenient resource available at all times is the online customer portal.

Synopsys Software Integrity Community

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

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

Access the Customer Success Community. If you do not have an account or have trouble accessing the system, click here to get started, or send an email to community.manager@synopsys.com.

Training

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

New videos and courses are added monthly.

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

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

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

Chapter 1: Announcements for Version 2021.4.0

New containers and changes to system requirements

In the 2021.6.0 release:

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

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

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

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

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

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

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

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

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

Retention period for unmapped code locations

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

Deprecated APIs

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

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

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

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

New job implementation in 2021.6.0 release

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

- `GET /jobs/{jobID}`

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

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

- `PUT /jobs/{jobID}`

  This call reschedules a job.

- `DELETE /jobs/{jobID}`

  This call terminates a job.

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

Japanese language

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

Notice for Azure customers

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

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

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

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

Deprecation of PostgreSQL version 9.6 for external databases

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

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

Internet Explorer 11 no longer supported

Synopsys has ended support for Internet Explorer 11.

Deprecated page

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

Japanese language

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

New containers and changes to system requirements

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

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

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

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

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

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

Ending support for Internet Explorer 11

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

Japanese language

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

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.

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.

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.

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.

Individual file matching

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

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

Upgrading to 2020.2.0 will turn individual file matching off and may cause some components to drop off the BOM. To estimate the impacts to your BOM, please look for components with only the match type of “Exact File” to see components that may drop from your BOM. Please note, if you are scanning docker images, “Exact File” matches are not impacted by this change.

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

Docker Compose support

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

Version 2021.4.2

Fixed Issues in 2021.4.2

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

- (Hub-28777) Fixed issue with the Project Version BOM Status not appearing in the Project Header.
- (Hub-29471) Fixed issue by changing query to alleviate the performance issue.

Version 2021.4.1

New and Changed Features in Version 2021.4.1

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

Fixed Issues in 2021.4.1

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

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

Version 2021.4.0

New and Changed Features in Version 2021.4.0

Rapid Scanning - Limited Customer Availability feature

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

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

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

Duplicate BOM detection

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

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

Ability to configure Project Manager role

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

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

Multi-license editing enhancements

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

Deep license data enhancement

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

Report enhancements

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

Policy management enhancements

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

Vulnerability Impact enhancement

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

Changes to LDAP or SAML group synchonization

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

Container enhancement

A health check was added to the Binaryscanner container.

Enhancement to the Source tab

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

Component and project search enhancement

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

Saved search enhancement

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

Performance improvement to the *Project Name* page

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

Cloning enhancements

The following enhancements were made to cloning a project version:

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

License conflicts enhancement

Manual edits to a BOM, including changing the usage for a component or the license of the project version using the **License Conflicts** or **Components** tab will now trigger a recalculation of the license conflict.

Enhancements to the System Information page

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

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

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

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

Removal of installation guides

The *Installing Black Duck using Kubernetes* and the *Installing Black Duck using OpenShift* guides have been

removed from the documentation set. These documents only contained links to the latest documentation. These links have been added to the Black Duck documentation page in each PDF and to the home page of the online help.

Enhancement to the *Project Name* page

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

Enhancement to the Dashboard page

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

API enhancements

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

    `GET /api/settings/analysis`
  - Updating analysis settings

    `PUT /api/settings/analysis`
  - Reading branding settings

    `GET /api/settings/branding`
  - Updating branding settings

    `PUT /api/settings/branding`
  - Reading license review settings

    `GET /api/settings/license-review`
  - Updating license review settings

```
PUT /api/settings/license-review
```

- Reading role settings

```
GET /api/settings/role
```

- Updating role settings

```
PUT /api/settings/role
```

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

Supported browser versions

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

Container versions

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

Japanese language

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

Fixed Issues in 2021.4.0

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

- (Hub-24015, 26281). Fixed an intermittent permission denied error seen in the Black Duck user interface.
- (HUB-25116). Fixed an issue where red dots appeared in the Snippet View dialog box for a file encoded in UCS-2, rendering the text unreadable.
- (HUB-25549). Fixed an issue with `/api/uploads` where the created code location was not mapped to the project version when codeLocationName contained Japanese characters.
- (HUB-25550). Added BOM update information to a project version's activity/journal.
- (HUB-25605, 27618). Fixed an issue when using `/api/tokens/authenticate` to authenticate with an API token, where after the token expired, the HTTP client got redirected to the SAML provider page or an error occurred when generating PDF reports.
- (Hub-25993). Fixed an issue where a duplicate record caused the following error message to appear in the job runner log: 'A conflicting object already exists.'
- (Hub-26481). Fixed an issue where a page would refresh completely after saving a new remediation status.
- (HUB-26588). Fixed an issue where running a binary scan on android-studio-ide-201.7199119-windows.exe failed.
- (Hub-26695). Fixed an issue where scans took significantly longer during certain times of the day.
- (Hub-26897). Fixed an issue so that a 404 Not Found error code appears for invalid versions which are those not listed on the *Component Name* page.
- (Hub-26911). Fixed an issue where selecting an alternate snippet match incorrectly identified a component as having cryptography.
- (Hub-27159). Fixed an issue for policy rules using the 'Contributors in the past year', 'Commits in the past year' or 'New Version Count' component conditions. Although these conditions were defined to trigger a violation if the value was equal to 0, policy violations were triggered when the value was greater than 0 or a component had no commit history.

  Note: With this fix, new scans or rescans may remove some policy violations that were previously triggered.
- (Hub-27167). Fixed an issue whereby active users assigned to an inactive group with the Global Project Viewer role could see all projects in the Dashboard.
- (Hub-27175). Fixed an issue where the **Used count** value on the *Component Name* page was inaccurate as it was based on the number of component origins, not the component versions.
- (Hub-27282). Fixed an issue where the policy violation popup in the BOM occasionally got stuck open and could not be closed unless the page was refreshed.
- (Hub-27284, 27660). Fixed an issue where some dynamically linked components with a match type of transitive dependency were missing the match information in the **Source** column in the project

version BOM.

- (Hub-27287). Fixed an issue so that risk counts shown on the **Overview** tab on the *Project Name* page use component version values (as the BOM page does), instead of by component origin.
- (Hub-27293). Fixed an issue where components marked as Reviewed were noted as Unreviewed when the project was rescanned.
- (Hub-27306). Fixed an issue where components were listed in case sensitive order in the Notices Report.
- (Hub-27308). Fixed an issue where the Black Duck KB *Component Name* page did not correctly show the number of vulnerabilities after the license for a component version was changed.
- (Hub-27326). Fixed an issue whereby deleting the application ID using the project's **Settings** tab did not actually delete the application ID.
- (Hub-27613). Fixed an issue where the source files for binaries could not be navigated in the **Source** tab.
- (Hub-27961). Fixed the legends for the graphs on the Dashboard page so that they did not appear clickable.
- (Hub-27982). Fixed an issue where the binary scan only identified the first and last files in an MSI archive.
- (Hub-27985). Fixed an issue with the message that appears when Black Duck is building the BOM which would disappear when you scrolled down the BOM page.
- (Hub-28094). Fixed an issue where the `/api/usergroups` endpoint was not properly using "_" or "%" in the search term.
- (Hub-28165). Fixed an issue with editing a license on the BOM page where selecting Cancel/Close still applied the changes.
- (Hub-28208). Fixed an issue where the code base size shown on the Registration page was incorrect.
- (Hub-28226). Fixed an issue so that components that are in violation of one or more policies will now generate a "policy cleared" notification when the code location that brought them in is unmapped or deleted.
- (Hub-28259). Fixed an issue with an unreview/unignore SQL query analysis.
- (Hub-28292). Fixed an issue where the HELM t-shirt sizing `.yml` files did not scale the BOM engine container.
- (Hub-28370). Fixed an issue where critical vulnerabilities were not shown when using the comparison view of the BOM.
- (Hub-28375). Fixed an issue so that the **Affected Projects** tab for a CVE or BDBA record no longer displays vulnerabilities from components that have been ignored.
- (Hub-28383). Fixed an issue where if the *Project Name* page was filtered and as a result only one version appeared on the page, the version could not be deleted.
- (Hub-28416). Fixed an issue where the AND or OR operator for a group of licenses could not be modified.
- (Hub-28458). Fixed an issue where the SnippetScanAutoBom job displayed an "Error in job execution: Duplicate key" error message.
- (Hub-28562). Fixed an issue with a binary scan where the scan failed to complete post work and the

following error message appeared: "Path is not a parent of null."

- (Hub-28580). Fixed an issue when attempting to access the **My Access Tokens** page caused the following error "The application has encountered an unknown error."
- (Hub-28639). Fixed an issue where the suffix of the downloaded report file had a `.json` extension instead of `.zip` if the project name contained both English and Chinese characters.
- (Hub-28681). Fixed an issue so that the usage is shown on the **Source** tab when the match type is direct or transitive dependency.
- (Hub-28765). Fixed an issue where the BOM page displayed snippets that were both confirmed and ignored.
- (Hub-28773). Fixed an issue so that TLSv1.1 was removed from the TLS_PROTOCOLS option in the `hub-webserver.env` file.

Version 2021.2.1

New and Changed Features in Version 2021.2.1

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

Fixed Issues in 2021.2.1

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

- (Hub-23928). Fixed an issue where a confirmed snippet match was changed after a rescan.
- (Hub-26898). Fixed an issue whereby a scan appeared to be completed, however, Synopsys Detect timed out as it failed to get a bom_complete notification from Black Duck.
- (Hub-27688). Fixed an issue whereby the API call for matched files returned no information for transitive and direct dependency matches.
- (Hub-28410). Fixed an issue where the RabbitMQ container could not be started on Kubernetes which was resolved by introducing a persistent volume.
- (Hub-28208, 28386). Fixed an issue whereby the incorrect code base size was displayed on the Product Registration page.
- (Hub-28278). Fixed an issue where a missing persistent volume for RabbitMQ container caused excessive logging in the BOM Engine and scan failures.
- (Hub-28292). Fixed an issue with scaling the BOM Engine container.

Version 2021.2.0

New and Changed Features in Version 2021.2.0

New custom vulnerability dashboards

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

Dashboard page to view dashboards from those saved searches.

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

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

Vulnerability search enhancements

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

The following attributes are available when searching for vulnerabilities:

- Affecting projects
- Default Remediation
- Reachable
- Exploit
- First Detected
- Remediation Status
- Solution
- Base Score
- Exploitability Score
- Impact Score
- Overall Score
- Published Year
- Severity
- Source (BDSA or NVD)
- Temporal Score
- Workaround

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

Ability to manage license conflicts for projects

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

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

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

Dependencies

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

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

Report database enhancements

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

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

- `license_ok_count`. Number of no license risk.
- `operational_high_count`. Number of high operational risk.
- `operational_medium_count`. Number of medium operational risk.
- `operational_low_count`. Number of low operational risk.
- `operational_ok_count`. Number of ok operational risk.

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

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

License editing enhancements

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

- When editing a license for a component, Black Duck now gives you the ability to easily create new or edit existing multi-license scenarios for the components in your BOM at the root level or at the same level as the original license.
- If you selected a different license for a component, you can now revert the license to its original license as defined in the Black Duck KnowledgeBase.
- A new option in the *Component Name Version* Component License dialog box makes it easily discernible that there is an edit mode.

Report enhancement

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

Notices File Report

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

Binary scan enhancement

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

Deep license data enhancement

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

BOM Engine

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

Black Duck tutorials

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

Modification to password configuration

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

Policy rule enhancement

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

Hosting location for Synopsys Detect

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

Saved search dashboard enhancements

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

Snippet triage enhancement

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

Supported browser versions

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

Container versions

- blackducksoftware/blackduck-postgres:1.0.16
- blackducksoftware/blackduck-authentication:2021.2.0
- blackducksoftware/blackduck-webapp:2021.2.0
- blackducksoftware/blackduck-scan:2021.2.0
- blackducksoftware/blackduck-jobrunner:2021.2.0

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

Supported Docker versions

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

Docker webapp-volume

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

API enhancements

- API documentation is now only available at https://<Black Duck server URL>/api-doc/public.html.
- Added the capability to filter code locations (/api/codelocations) by creation date.
- Fixed the API used to download the SAML Identity Provider Metadata XML file (api/sso/idp-metadata endpoint) that was working incorrectly in previous versions.
- The remediation-guidance endpoint (GET /api/components/{componentId}/versions/{componentVersionId}/remediating) no longer returns a “410 GONE” response. You must switch to the upgrade-guidance endpoint, (GET /api/components/{componentId}/versions/{componentVersionId}/upgrade-guidance) which is incompatible with the remediation-guidance endpoint that was removed.
- Added a report dependency-paths endpoint to show dependency paths for a component:

  /api/project/{projectId}/version/{projectVersionId}/origin/{originId}/dependency-paths
- Added the Synopsys Detect URI endpoint which is only used to set or update reading the Synopsys Detect URI on the System Settings page:

  /external-config/detect-uri

Ubuntu operating system

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

Japanese language

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

Fixed Issues in 2021.2.0

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

- (Hub-22103). Fixed an issue whereby the Black Duck server did not respond in time when updating a license status.
- (Hub-22623). Fixed an issue whereby the Summary Dashboard frequently timed out for enterprise customers when loading in the UI.
- (Hub-24332). Fixed an issue where scanning the same code location caused duplicated notifications.
- (Hub-25374). Fixed a permission error for database azure_maintenance.
- (Hub-25580). Fixed an issue whereby components shown in the BOM were incorrectly sorted after page 9.
- (Hub-25666). Fixed a pagination issue for the endpoint /usergroups/<group #>/roles.
- (Hub-26030). Fixed an issue where sorting options were not retained for a dashboard by project name after performing an action.
- (Hub-26324). Fixed an issue where the following error "java.lang.IllegalStateException: Parent of [file:/C:/src/External/PackageManager/ProjectTemplates/com.unity.template.universal-10.1.0.tgz] does not exist" occurred when uploading a scan.
- (Hub-26343). Fixed an issue where Black Duck could not be registered as the registration container ran out of heap space.
- (Hub-26493). Fixed a confusing error message which appeared when a user removed themselves as a member of a project.
- (Hub-26501). Fixed an issue whereby the cordova-plugin-inappbrowser component could not be selected in the Edit Component dialog box.
- (Hub-26536). Fixed an issue whereby a watched project displayed the Unwatched icon () in the page header.
- (Hub-26540). Fixed an issue whereby the initial configuration of SAML did not go into effect unless Black Duck was restarted.
- (Hub-26615). Fixed an issue whereby a user with the Project Manager role in Project A and Project Manager and Project Code Scanner roles in Project B could upload scans to Project A.
- (Hub-26616). Fixed an issue whereby attempting to ignore a snippet would fail with the following error message: "Unable to update existing snippet adjustment because changing the consumer, producer, adjustment type, start line, end line is not supported."
- (Hub-26712, 26962). Fixed an issue whereby the snippet icon shown in the tree view on the **Source** tab did not clear after a snippet match was confirmed.
- (Hub-26726). Fixed an issue whereby the "not in" option was not available for custom fields when creating a policy rule.
- (Hub-26807). Fixed an issue whereby a HTML status code 404 was received when attempting to GET custom fields for the BOM component version.
- (Hub-26815). Fixed an issue whereby saving SAML integration settings caused the page to reload and switch Identity Provider Metadata settings.
- (Hub-26904). Fixed an issue whereby the match count value shown on the project version **Activity**

section on the **Settings** tab was not the same as on the *Scan Name* page.

- (Hub-26930). Fixed an issue where notifications where not triggered for a component.
- (Hub-27002). Fixed an issue whereby the wrong notification was sent when a cloned project was created.
- (Hub-27049). Fixed an issue whereby the License Terms category for a Project Version Report could not be seen in the Black Duck UI without a user being assigned the License Manager role.
- (Hub-27208). Fixed an issue with blackduck-nginx whereby Synopsys Alert failed to load when SAML was configured.
- (Hub-27227). Fixed an issue whereby snippet matching took a long time to complete.
- (Hub-27264). Fixed an issue whereby reviewing a component reset its usage to its default value.
- (Hub-27681). Fixed an issue whereby the BOM Engine had to be started by a root user when deployed on Kubernetes with a custom security context.

Version 2020.12.0

New and Changed Features in Version 2020.12.0

New containers and changes to system requirements

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

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

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

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

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

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

Password configuration

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

Super Users can:

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

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

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

License enhancements

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

Vulnerability Impact Analysis enhancements

- A new project version report, `vulnerability_matches_date_time.csv`, has been added. It lists the component, vulnerability data, and vulnerability impact analysis data for each component potentially reached by a vulnerability. This report has the following columns:
  - Component name
  - Component id
  - In use
  - Component version name
  - Version id
  - Channel version origin
  - Origin id
  - Origin name id
  - Vulnerability Id
  - Vulnerability source
  - CVSS Version
  - Security Risk
  - Base score
  - Overall score
  - Solution available
  - Workaround available
  - Exploit available
  - Called Function
  - Qualified Name
  - Line Number

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

BOM computation information

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

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

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

Policy enhancements

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

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

Report enhancements

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

Configuration of snippet file size

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

Configuration of the clean up of unmapped code locations

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

Access tokens

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

Supported browser versions

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

  Note that support for Internet Explorer 11 is deprecated and Synopsys will be ending support for Internet Explorer 11 starting with the Black Duck 2021.2.0 release.
- Microsoft Edge 87.0.664.60 (Official build) (64-bit)

Container versions

- blackducksoftware/blackduck-postgres:1.0.16
- blackducksoftware/blackduck-authentication:2020.12.0
- blackducksoftware/blackduck-webapp:2020.12.0
- blackducksoftware/blackduck-scan:2020.12.0
- blackducksoftware/blackduck-jobrunner:2020.12.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.8
- blackducksoftware/blackduck-registration:2020.12.0
- blackducksoftware/blackduck-nginx:1.0.26
- blackducksoftware/blackduck-documentation:2020.12.0
- blackducksoftware/blackduck-upload-cache:1.0.15
- blackducksoftware/blackduck-redis:2020.12.0
- blackducksoftware/blackduck-bomengine:2020.12.0

- sigsynopsys/bdba-worker:2020.09-1
- blackducksoftware/rabbitmq:1.2.2

API enhancements

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

  GET /api/projects/{projectId}/versions/{projectVersionId}/vulnerabilities/{vulnerabilityId}/vulnerability-matches
- Added the following BOM endpoints:
  - Get BOM status summary:

    GET /api/projects/{projectId}/versions/{projectVersionId}/bom-status
  - List a BOM's events:

    GET /api/projects/{projectId}/versions/{projectVersionId}/bom-events
  - Delete a failed BOM event:

    DELETE /api/projects/{projectId}/versions/{projectVersionId}/bom-events/{bomEventId}
  - Delete all failed events from a BOM:

    DELETE /api/projects/{projectId}/versions/{projectVersionId}/bom-events
- New password settings endpoints:
  - Get password settings:

    GET /api/password/security/settings
  - Get system password settings:

    GET /api/password/management/settings
  - Update system password settings:

    PUT /api/password/management/settings
  - Validate password:

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

Japanese language

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

Fixed Issues in 2020.12.0

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

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

Version 2020.10.1

New and Changed Features in Version 2020.10.1

Container versions

- blackducksoftware/blackduck-postgres:1.0.13
- blackducksoftware/blackduck-authentication:2020.10.1
- blackducksoftware/blackduck-webapp:2020.10.1
- blackducksoftware/blackduck-scan:2020.10.1
- blackducksoftware/blackduck-jobrunner:2020.10.1
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.8
- blackducksoftware/blackduck-registration:2020.10.1
- blackducksoftware/blackduck-nginx:1.0.26
- blackducksoftware/blackduck-documentation:2020.10.1

- blackducksoftware/blackduck-upload-cache:1.0.15
- blackducksoftware/blackduck-redis:2020.10.1
- sigsynopsys/bdba-worker:2020.09-1
- blackducksoftware/rabbitmq:1.2.2

Fixed Issues in 2020.10.1

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

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

Version 2020.10.0

New and Changed Features in Version 2020.10.0

New custom component dashboards

So that you can easily view the component versions that are important to you, in 2020.10.0, the Component Dashboard has been replaced with custom component dashboards based on your saved component searches. Black Duck now provides the ability for you to search for components used in your projects using a variety of attributes, save the search, and then use the Dashboard page to view dashboards from those saved searches.

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

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

Component and Black Duck KnowledgeBase search enhancements

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

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

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

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

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

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

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

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

Enhancement to saved searches

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

License conflicts

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

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

License Management Enhancements

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

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

New component usage

Black Duck has added an "Unspecified" usage which you can use to indicate that you need to investigate the usage of the component. You may find it useful to use this usage as the default value instead of existing defaults such as Dynamically Linked to eliminate confusion about whether the component is assigned its true usage value or the default value.

New tier

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

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

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

There is no change to the existing tiers.

Enhancements to custom fields

The following enhancements have been made to custom fields

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

Allowed signature lists

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

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

Enhancements to vulnerability impact analysis

The following enhancements have been made to vulnerability impact analysis:

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

Report enhancements

The following reports have been enhanced:

- A new column, "Comments", has been added to the end of the `components_date_time.csv` project version report and lists the comments for each component.
- A new column, "Match type", has been added to the end of the `vulnerability-status-report_date_time.csv` report to identify the match type.

Enhancements to the Report Database

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

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

HTTP/2 and TLS 1.3

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

support HTTP/1.1 and TLS 1.2.

Change to jobs for purging scans

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

API enhancements

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

  GET /api/sso/status

- Added endpoints for retrieving SAML/LDAP configurations (Admin use only).
  - Read SSO configuration:

    GET /api/sso/configuration

  - Download an IDP metadata file:

    GET /api/sso/idp-metadata

  - These SSO endpoints were also added:
    - Update SSO configuration:

      POST /api/sso/configuration

    - Upload an IDP metadata file:

      POST /api/sso/idp-metadata

- Added the following BOM hierarchical component endpoints:
  - List hierarchical root components:

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

  - List hierarchical children components:

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

  - List hierarchical children component versions:

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

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

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

- eventSource

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

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

Supported browser versions

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

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

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

Container versions

- blackducksoftware/blackduck-postgres:1.0.13
- blackducksoftware/blackduck-authentication:2020.10.0
- blackducksoftware/blackduck-webapp:2020.10.0
- blackducksoftware/blackduck-scan:2020.10.0
- blackducksoftware/blackduck-jobrunner:2020.10.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.6
- blackducksoftware/blackduck-registration:2020.10.0
- blackducksoftware/blackduck-nginx:1.0.26
- blackducksoftware/blackduck-documentation:2020.10.0
- blackducksoftware/blackduck-upload-cache:1.0.15
- blackducksoftware/blackduck-redis:2020.10.0
- sigsynopsys/bdba-worker:2020.09
- blackducksoftware/rabbitmq:1.2.2

Japanese language

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

Fixed Issues in 2020.10.0

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

- (Hub-20559, 22100). Fixed an issue where snippet adjustments were lost when scanning the same code location from a different root directory or when cloning a project version.
- (Hub-21421). Fixed an issue where the print functionality did not work for large projects.
- (Hub-23705, 25560). Fixed an issue where users could not delete reports that they created.
- (Hub-23709). Fixed an issue whereby the following scan.cli.sh warning message appeared when scanning: "Unable to find manifest from all manifests."
- (Hub-24330). Fixed an issue whereby an error message ("Duplicate key value violates unique constraint") appeared when importing a Protex project into Black Duck version 2019.10.3.
- (Hub-24673). Fixed an issue whereby navigating from a Dashboard page failed if there were more than 32,000 components.
- (Hub-24675). Fixed an issue whereby the root_bom_consumer_node_id was set incorrectly
- (Hub-24871). Fixed an issue with PostgreSQL database growth since release 2019.10.0.
- (Hub-24772). Fixed an issue where the default `.pdf` filename when printing a BOM was not the project name and version name.
- (Hub-24839). Fixed an issue where some component origin IDs could not be selected from the Add/Edit Component dialog box.
- (Hub-24947). Fixed an issue whereby search results when adding a project to a BOM were listed inconsistently.
- (Hub-25171). Fixed an issue whereby the vulnerability count was not updated when remediated using an API until after a rescan (PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/origins/{originId}/vulnerabilities/{vulnerabilityId}/remediation).
- (Hub-25219). Fixed an issue with creating reports through the API, wherein specifying a locale such as "locale" : "ja_JP" was ignored. Now, the locale field correctly sets the language of the generated report.
- (Hub-25234). Fixed an issue where the **Print** button to print a BOM was occasionally missing bar graph counts.
- (Hub-25240). Fixed an issue where browser or API calls for a specific vulnerability (BDSA-2020-1674) failed.
- (Hub-25241). Fixed an issue where the VersionBomComputationJob failed for scans with the following error message: "Data integrity violation (Constraint:not_null, Detail: on column source_start_lines)".
- (Hub-25244). Fixed an issue whereby manually added components were deleted from the BOM after upgrading to Black Duck release 2020.4.2.
- (Hub-25247). Fixed an issue whereby the following error message appeared in the Black Duck PostgreSQL logs: "ERROR: duplicate key value violates unique constraint "scan_component_scan_id_bdio_node_id_key".
- (Hub-25321). Fixed an issue where when scrolling the BOM page, text appeared in areas on the page where text should not appear.
- (Hub-25324). Fixed an issue where the Scan *Name* page did not word wrap.
- (Hub-25478). Fixed an issue where the security risk filter on the Security page became invisible.
- (Hub-25508). Fixed an issue where old media types (v4 and v5) did not always work for the policy

rules API (GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/policy-rules).

- (Hub-25522, 25523). Fixed an issue where formatting issues appeared in the BOM print preview window in Chrome for Black Duck version 2020.8.0.
- (Hub-25548). Fixed an issue where selecting new component matches in the hierarchical view did not update component matches in the Source view.
- (Hub-25570). Fixed an issue whereby the Security Dashboard page only partially loaded.
- (Hub-25608). Fixed an issue where vulnerabilities were counted twice in the "New Vulnerabilities" and "New Remediated Vulnerabilities" categories in the Vulnerability Update report.
- (Hub-25649). Fixed an issue where the policy violation popup windows on the Dashboard page would not close.
- (Hub-25841). Fixed an issue whereby numbers entered into a custom field of type Text were converted into a date format.

Version 2020.8.2

New and Changed Features in Version 2020.8.2

Black Duck version 2020.8.2 is a maintenance release and contains no new or changed features.

Fixed Issues in 2020.8.2

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

- (Hub-24871). Fixed an issue with PostgreSQL database growth since release 2019.10.0.
- (Hub-25967). Fixed an issue whereby the usage of a component could not consistently be modified.

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 URIs (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 KnowedgeBase 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.

Chapter 3: Known Issues and Limitations

No known issues and limitations to report in Black Duck