




Getting Started

Version 2020.10.0



This edition of the *Getting Started* refers to version 2020.10.0 of Black Duck.

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

Please send your comments and suggestions to:

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

Copyright © 2020 by Synopsys.

All rights reserved. All use of this documentation is subject to the license agreement between Black Duck Software, Inc. and the licensee. No part of the contents of this document may be reproduced or transmitted in any form or by any means without the prior written permission of Black Duck Software, Inc.

Black Duck, Know Your Code, and the Black Duck logo are registered trademarks of Black Duck Software, Inc. in the United States and other jurisdictions. Black Duck Code Center, Black Duck Code Sight, Black Duck Hub, Black Duck Protex, and Black Duck Suite are trademarks of Black Duck Software, Inc. All other trademarks or registered trademarks are the sole property of their respective owners.

| | |
|---|-----------|
| Chapter 1: Logging in to Black Duck | 1 |
| Chapter 2: Scanning your code | 3 |
| Using Synopsys Detect (Desktop) | 3 |
| Downloading and installing Synopsys Detect (Desktop) | 3 |
| Configuring Synopsys Detect (Desktop) | 4 |
| Certificates | 10 |
| Scanning options | 10 |
| Creating a scan file | 14 |
| Managing scans | 15 |
| Uploading scan files to Black Duck | 17 |
| Viewing uploaded scans | 18 |
| Creating a project | 20 |
| Mapping a scan to a project | 21 |
| Chapter 3: Viewing risk in Black Duck | 23 |
| Dashboards | 23 |
| Project version pages | 27 |
| Viewing your dashboards | 28 |
| Viewing dashboards | 29 |
| About the Watching and My Projects dashboards | 29 |
| About saved searches dashboards | 33 |
| Viewing the health of your projects | 40 |
| About security risk | 42 |
| Suggested work flow | 43 |
| Viewing all security vulnerabilities | 44 |
| Chapter 4: Viewing your BOM | 46 |
| Adjusting the component and/or component version in a BOM | 46 |
| Selecting a different license for a component in a BOM | 48 |

Black Duck documentation

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

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

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

Customer support

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

You can contact Synopsys Support in several ways:

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

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

Synopsys Software Integrity Community

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

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

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

Training

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

New videos and courses are added monthly.

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

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

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

Chapter 1: Logging in to Black Duck

Black Duck is a risk management tool designed to help you manage the logistics of using open source software in your organization.

Using Black Duck, you can:

- Scan your code and identify open source software that exists in your code base.
- View the generated Bill of Materials (BOM) for your software projects.
- View vulnerabilities that have been identified in open source components.
- Assess your security, license, and operational risk.

Logging in to Black Duck lets you search projects that may be restricted to team members or company employees.

Note: You must have a username and password to access Black Duck. Contact your system administrator if you do not have a username. If Black Duck is configured to use LDAP, you may be able to log in to Black Duck using those credentials.

To log in to Black Duck

1. Using a browser, navigate to the Black Duck URL supplied by your system administrator. Typically the URL is in the format `https://<server hostname>`.
2. Enter the username and password provided by your Black Duck administrator.

Note: Your password is case sensitive.

3. Click **Login**.

When you first log in after installing Black Duck, an empty Dashboard page appears. For information to appear in Black Duck, you need to scan your code and map your code to a project, as described in the next chapter.

The screenshot shows the Black Duck Dashboard interface. At the top, there's a navigation bar with 'Dashboard', 'Security', and 'Summary' tabs. Below this, there are tabs for 'Watching' and 'My Projects'. A message states: 'Saved Searches: No saved searches? No problem, head over to find, query the data you're interested in and save the query for future use.' Below this, there's a 'Sort By...' dropdown and a 'Filter projects...' input field. The main content area features a large circular graphic with the text 'You don't have any projects' and a sub-message: 'Looks like you haven't created any projects nor have permission to see others. Click Create at the top to begin your journey to better code!'. To the right, there's a 'My Projects' section showing '0 Projects'. Below this, there are four risk categories: 'Policy Violations', 'Security Risk', 'License Risk', and 'Operational Risk'. Each category has a list of risk levels with corresponding percentages: '0% Blocker', '0% Critical', '0% Major', '0% Minor', '0% Trivial', '0% Unspecified' for Policy Violations; '0% Critical', '0% High', '0% Medium', '0% Low' for Security Risk; '0% High', '0% Medium', '0% Low' for License Risk; and '0% High', '0% Medium', '0% Low' for Operational Risk. At the bottom right, it says 'Displaying 1-0 of 0'.

By default the Dashboard page only shows the **Watching** and **My Projects** dashboards. You can also create custom dashboards so that you can quickly view the project versions or component versions that are important to you: search for projects and/or components and then save the searches. Your saved searches appear on the Dashboard page.

Black Duck component scanning is scanning functionality that provides an automated way to determine the set of open source software (OSS) components that make up a software project. Component scanning helps organizations manage their use of open source binaries by identifying and cataloging OSS components in order to provide additional metadata such as license, vulnerability, and OSS project health for those components.

Using Synopsys Detect (Desktop)

Synopsys Detect (Desktop) provides a new interface to make it easier to scan code.

With Synopsys Detect (Desktop), you can:

- [Scan](#) source directories, binaries and executables, and docker images and distributions.
- [Create a scan file](#) to be uploaded at a later time.
- [Manage scan files](#).
- [Upload scan files](#) directly to Black Duck.
- [View uploaded scans](#).

To use Synopsys Detect (Desktop):

1. Download and install Synopsys Detect (Desktop).
2. Configure Synopsys Detect (Desktop) with your Black Duck server settings and complete the installation process.
3. Use Synopsys Detect (Desktop) to scan and/or upload your files.

Note: An error message appears if you exceed the scan size limit, which is 5 GB (6 GB for Black Duck - Binary Analysis). Contact Customer Support if you receive this message.

Downloading and installing Synopsys Detect (Desktop)

1. Log in to Black Duck.
2. Navigate to the drop-down menu under your username and select **Tools**.
3. Select the operating system you wish to use in the **Downloads Synopsys Detect (Desktop)** section to download the executable from Google Cloud Storage.
4. Run the executable to install Synopsys Detect (Desktop).

If you are upgrading from a previous version of Synopsys Detect (Desktop), an option appears to migrate data from the previous version.

Note: As the application installs into a directory related to its name, Synopsys Detect (Desktop) will not uninstall previous versions of Black Duck Detect Desktop. It also will not uninstall versions of Synopsys Detect (Desktop) that were installed in a non-default directory. You must manually uninstall all previous versions of Black Duck Detect Desktop, versions of Synopsys Detect (Desktop) installed in the non-default directory, and fix or delete any shortcuts.

If the Synopsys Detect (Desktop) does not open after installation and the following error message appears:

```
The SUID sandbox helper binary was found, but is not configured correctly.
Rather than run without sandboxing I'm aborting now. You need to make sure
that /opt/Synopsys Detect/chrome-sandbox is owned by root and has mode
4755.
```

your operating system does not support the Sandbox at the kernel layer. To run Synopsys Detect (Desktop) with the Sandbox disabled, enter the following at the command line:

```
synopsys-detect --no-sandbox
```

Installing the Linux version of Synopsys Detect (Desktop)

1. Optionally, update all installed packages:

```
sudo yum update -y
```

2. Install a required library:

```
sudo yum install -y libXScrnSaver
```

3. Download `synopsys-detect-latest.rpm` from your Black Duck server, as described in the previous section.

4. Install Synopsys Detect (Desktop):

```
cd Downloads
sudo rpm -ivh synopsys-detect-latest.rpm
```

5. Change the permission of chrome-sandbox:

```
cd "/opt/Synopsys Detect"
sudo chmod 4755 chrome-sandbox
```

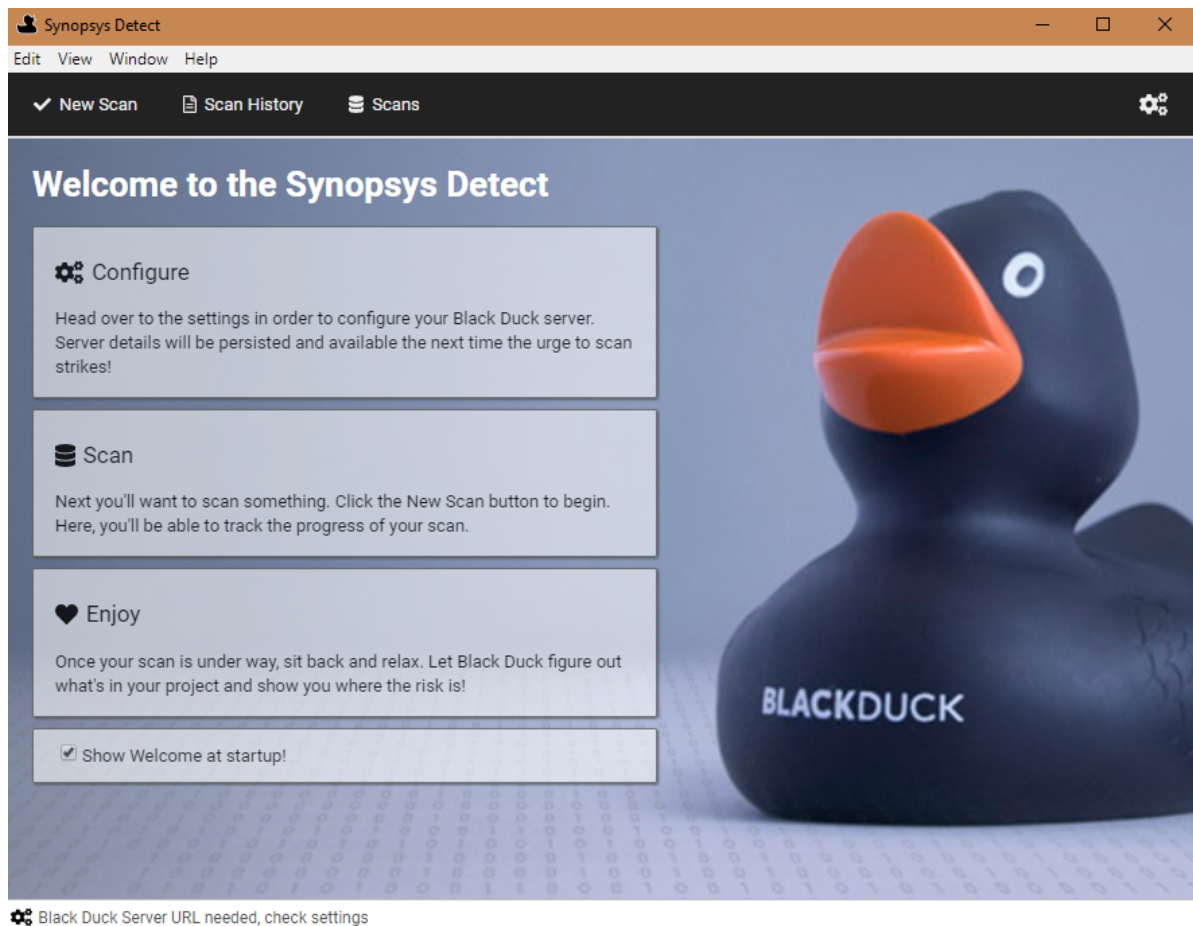
6. Run Synopsys Detect (Desktop):

```
./synopsys-detect --no-sandbox
```

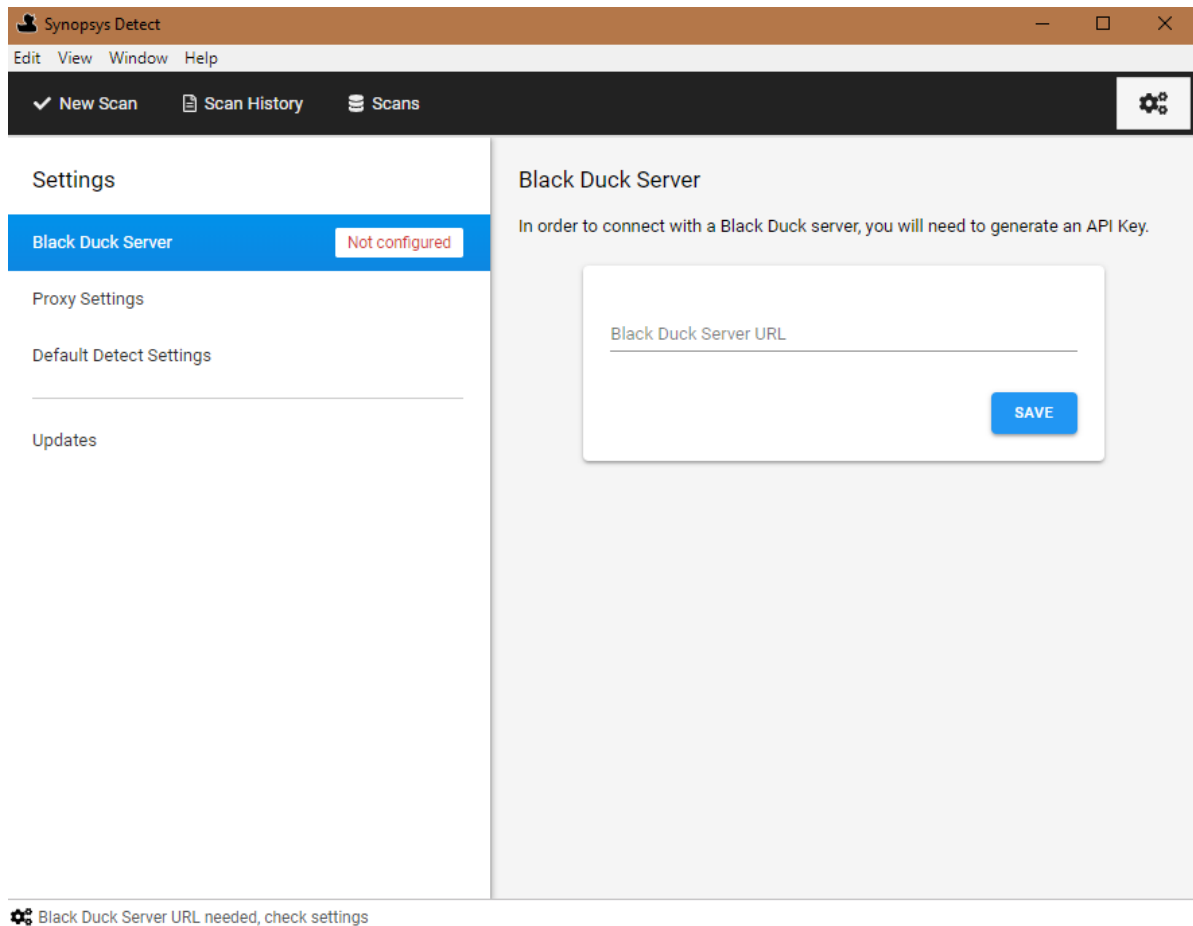
Configuring Synopsys Detect (Desktop)


After installing Synopsys Detect (Desktop), continue the installation process by configuring your Black Duck settings.

1. After installing or upgrading to Synopsys Detect (Desktop), the Welcome page appears.



2. Select **Configure** to display the Settings page.



You can also click , located in the upper right corner, to display this page.

3. As described below, select one of the following tabs and complete the installation and configuration process:
 - Black Duck Server
 - Proxy Settings
 - Default Detect Settings
 - Updates

Black Duck server settings

1. Specify the Black Duck Server URL. Enter the URL to the Black Duck server as you would type it in the browser, for example `https://servername:8443/`

If required, enter context information, for example, if the X-Forwarded-Prefix header is being specified in a proxy server/load balancer configuration.

2. Click **Save**. Synopsys Detect (Desktop) connects to the Black Duck server and displays the version of Black Duck you are connected to.


3. Generate or enter an API key (user access token). This information appears after you enter the Black Duck Server URL.
 - To generate a new API key:
 - a. Select **Generate New API Key**.
 - b. Enter a key name, your username, and password.
 - c. Click **Generate**.
 - To enter an API key:
 - a. Select **Enter API Key**.
 - b. Enter the API key in the field.
 - c. Click **Save**.

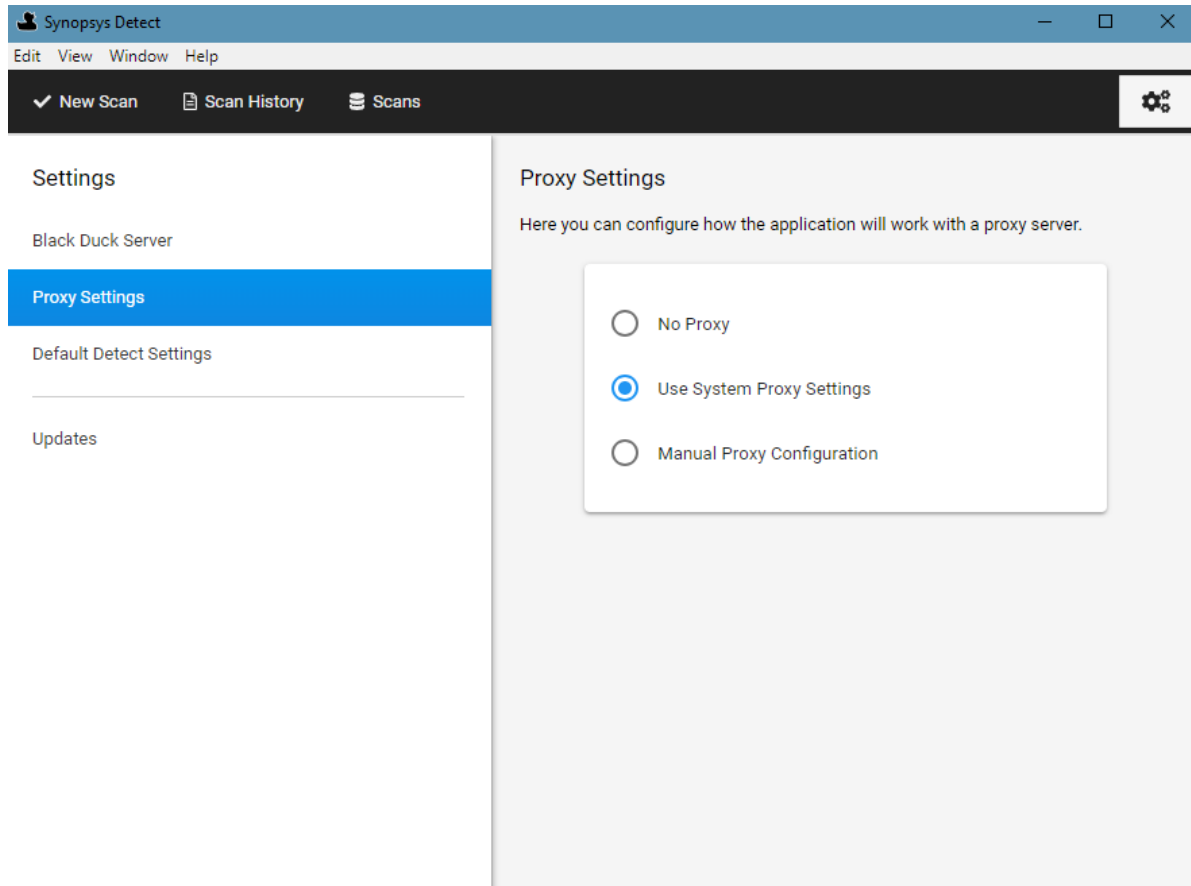
Proxy settings

Accessing Synopsys Detect (Desktop) through a proxy is supported. Synopsys Detect (Desktop) automatically uses your local system proxy setup.

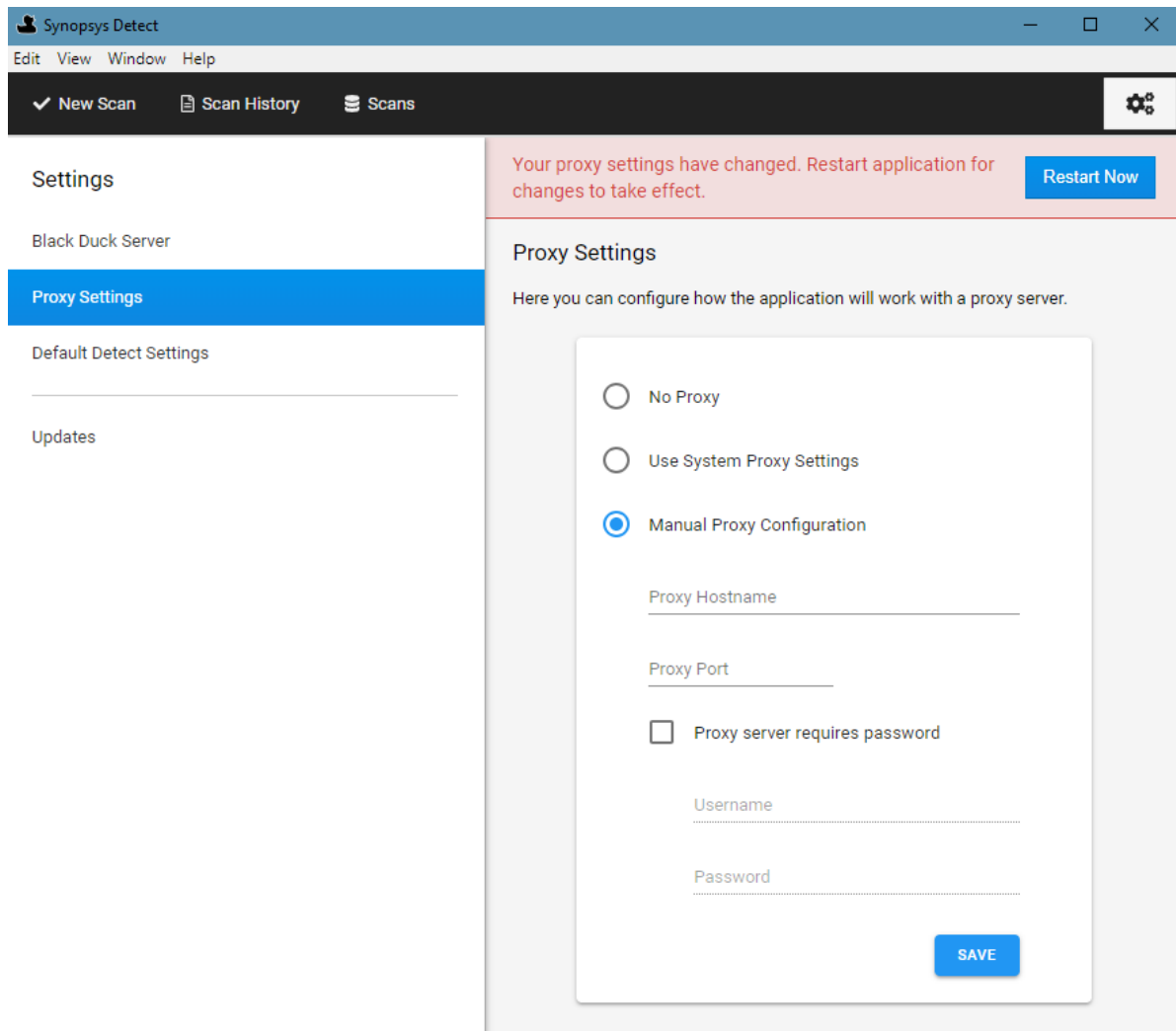
If you are required to manually enter your proxy settings or you do not require a proxy, you can modify these default settings.

⚙️ To modify the default proxy settings

1. Click  to display the Settings page and select the **Proxy Settings** tab.



2. Select either **No Proxy** or **Manual Proxy Configuration**.
3. If you select a manual proxy configuration:



- a. Enter the following information:
 - Your proxy host name.
 - Port number.
 - Whether authentication is required.
 - Your username and password.

If a proxy is enabled and authentication is required, you may have to re-enter your username and password.

- b. Click **Save**.
4. Restart the application.

Configuring Synopsys Detect settings

Optionally, select **Default Detect Settings** and if necessary, define any Synopsys Detect settings, clear any build tools you do not want to use, or manually configure the path to the build tools.

Checking for updates

You can check to see if there are updates to the Synopsys Detect (Desktop) by selecting the **Updates** tab. The page lists the last time you checked for updates. Click **Check for updates** to view if there are newer versions available. This option is only available for Windows and MacOS systems.

Certificates

When connecting to Black Duck: if you connect to a Black Duck instance with an insecure SSL certificate, you are prompted to view and trust the certificate. Select the **Always trust <Black Duck instance server name> to trust** option.

Note: On the Mac OS, even though you have accepted the certificate, your key store may display more options than were originally presented. For the SSL certificate, you must select the *Always trust* option. This prevents future prompts asking you about trusting certificates.

Scanning options

The Synopsys Detect (Desktop) makes it easier to scan:

- Source directories
- Binaries or executables
- Docker images or distributions

By default, all scans are uploaded to the Black Duck server and mapped to a project version. However, you can create a scan file as described [here](#), to output the scan to a file which you can later upload to Black Duck.

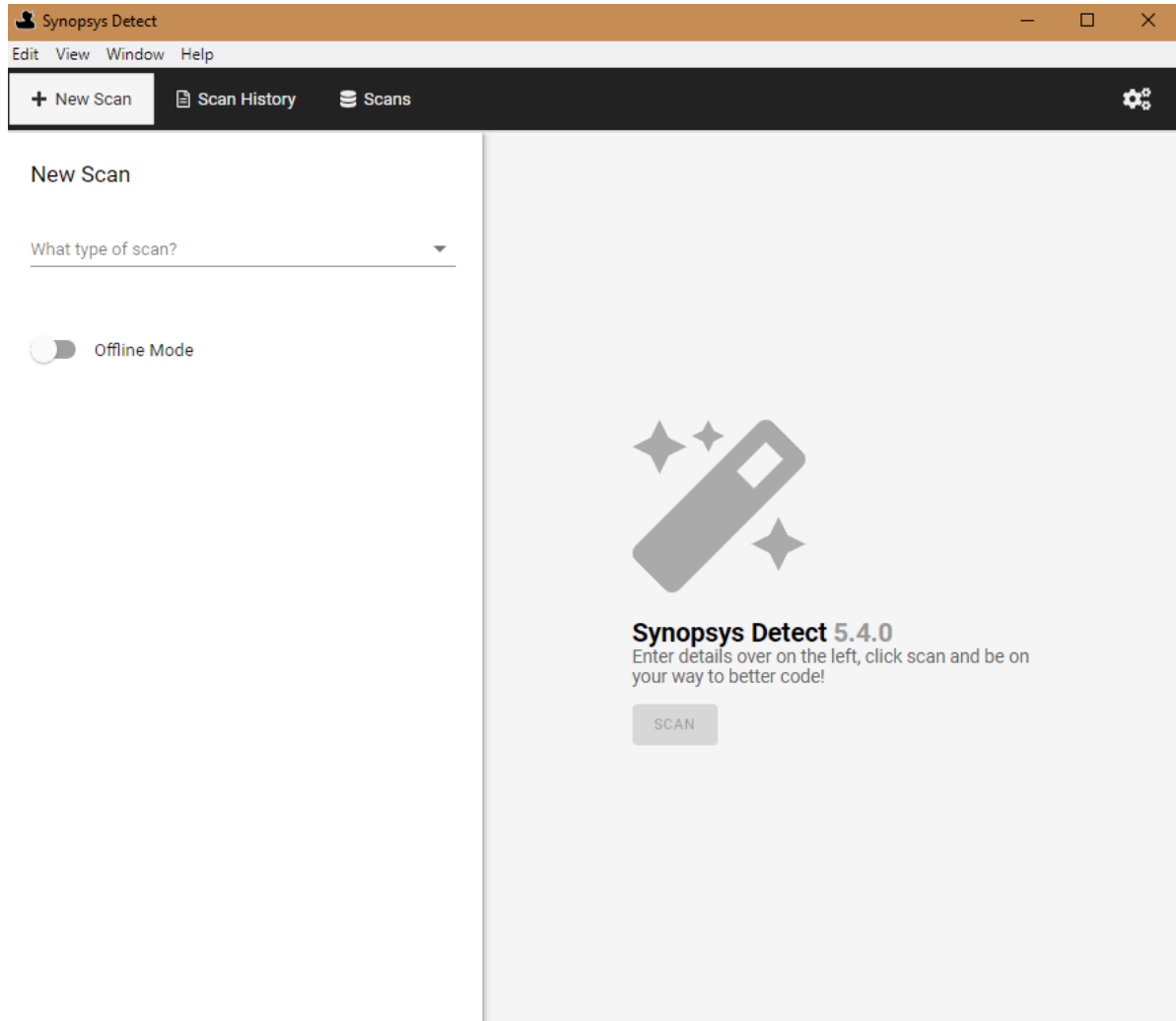
To specify project and/or version names:


1. Click **ADD** located next to **Project Settings**.
2. Select **Project Name** and/or **Version Name**. The fields appear in the UI.
3. Specify the values for the field(s).

Scanning Source Directory

⚙️ To scan a source directory

1. Click **New Scan**.



2. From the **What type of scan?** list, select **Source Directory**,
3. Click  to select the directory you would like to scan.
4. Optionally, modify or configure any project or scan settings by clicking **ADD** and selecting the setting.
If you have purchased a snippet scanning license and want to enable snippet scanning, select **Snippet Scanning** from the **Settings** options and enable it.
5. Click **Scan**.

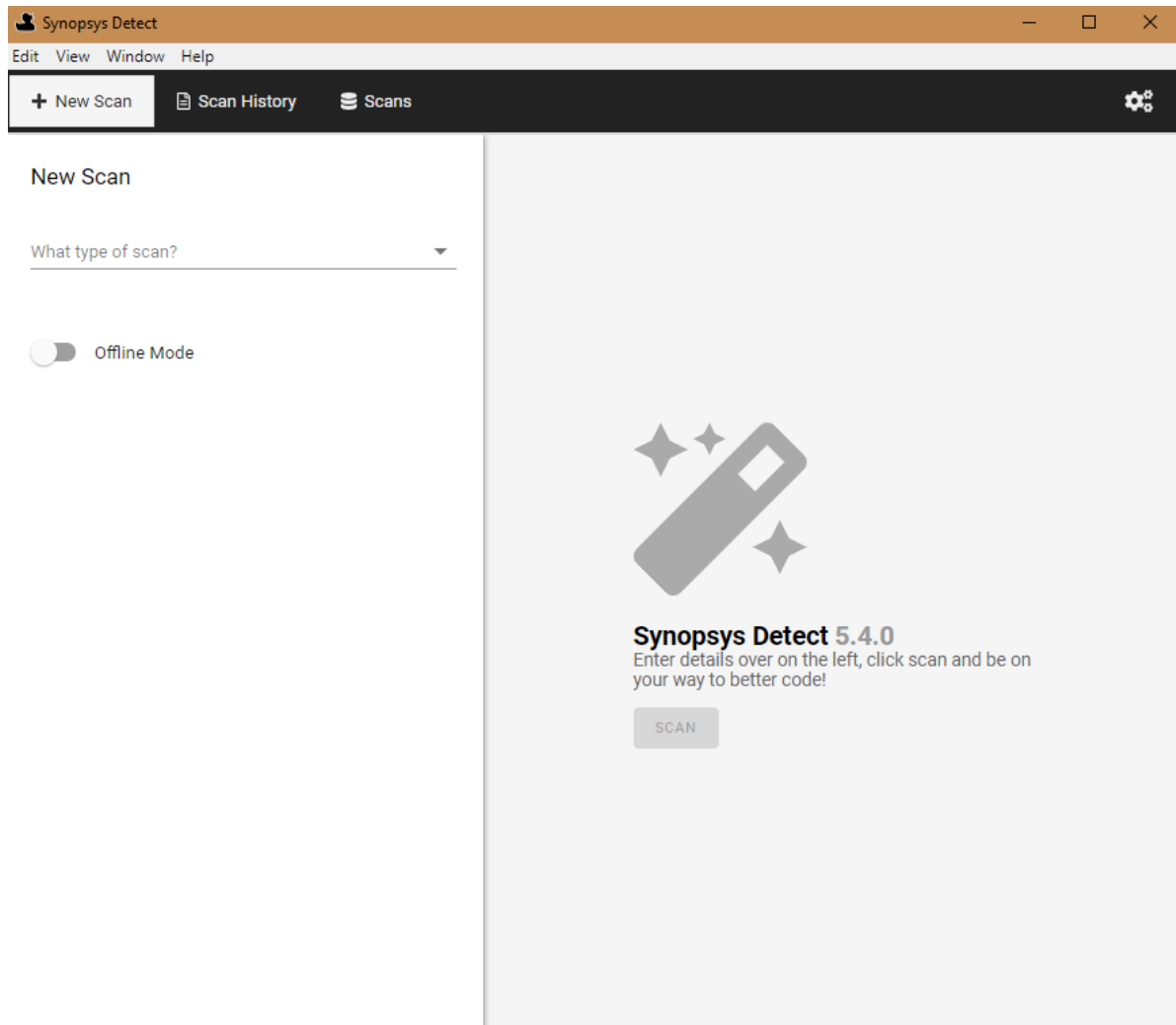
The status of the scan appears along with an option to cancel the scan.


- When the scan is complete, select the **Scan History** tab to view information on the completed scan. From this tab, you can [manage your scan](#). You can also view the uploaded scan using the **Scans** tab.

Scanning binary/executable

⚙️ To scan a single binary or executable

- Click **New Scan**.



- From the **What type of scan?** list, select **Binary/Executable**,
- Click  to select the binary or executable you would like to scan.
- Optionally, modify or configure any project settings by clicking **ADD** and selecting the setting.
- Click **Scan**.

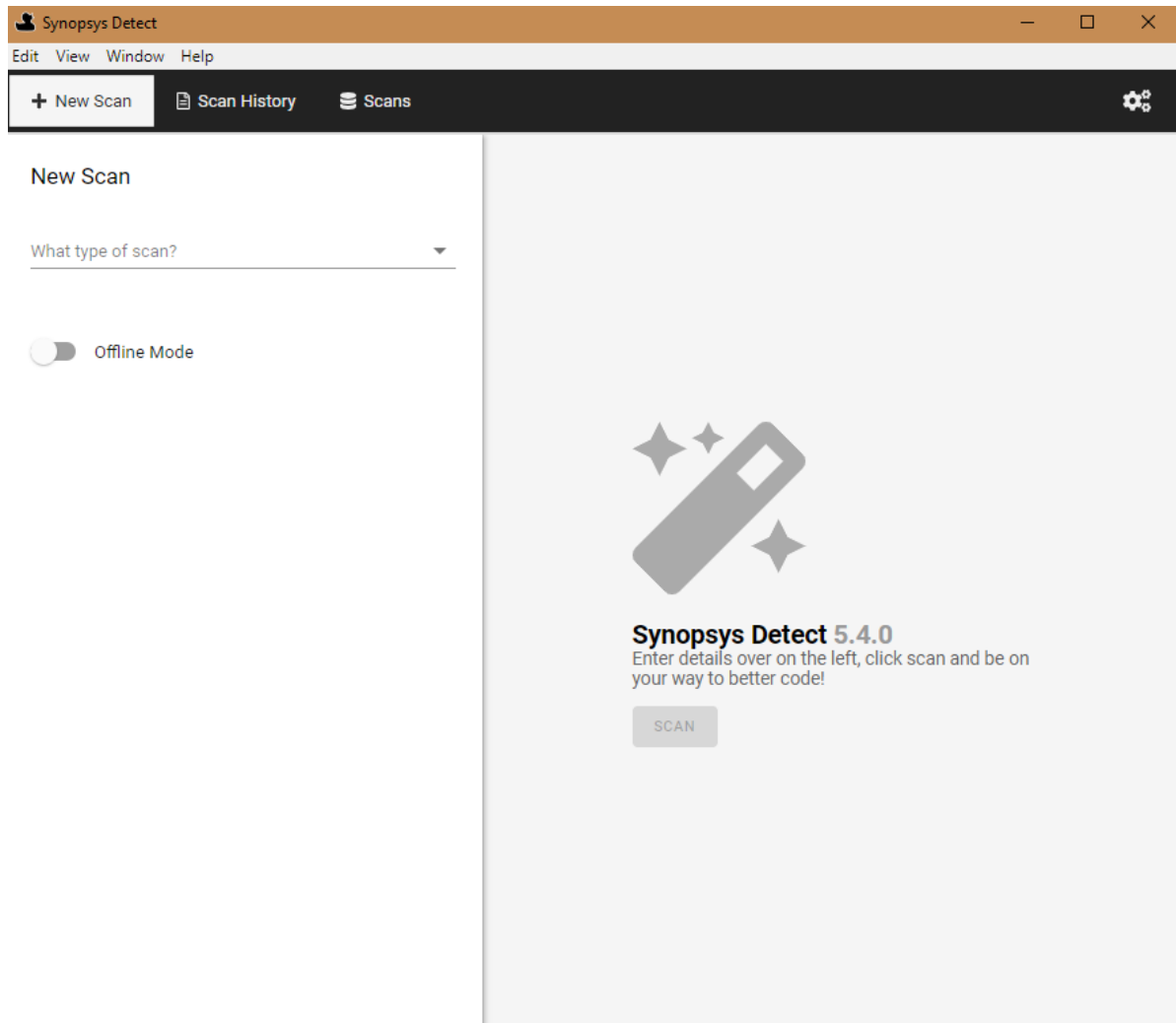
The status of the scan appears along with an option to cancel the scan.


- When the scan is complete, select the **Scan History** tab to view information on the completed scan. From this tab, you can [manage your scan](#). You can also view the uploaded scan using the **Scans** tab.

Scanning a Docker image or distribution

⚙️ To scan a Docker image or distribution (.tar file)

- Click **New Scan**.



- From the **What type of scan?** list, select **Docker**,
- Do one of the following:
 - Enter the Docker image name.
 - Select **Choose Docker File (.tar)** and click  to select the directory you would like to scan.
- Optionally, modify or configure any project settings by clicking **ADD** and selecting the setting.

5. Click **Scan**.

The status of the scan appears along with an option to cancel the scan.

6. When the scan is complete, select the **Scan History** tab to view information on the completed scan. From this tab, you can [manage your scan](#). You can also view the uploaded scan using the **Scans** tab.

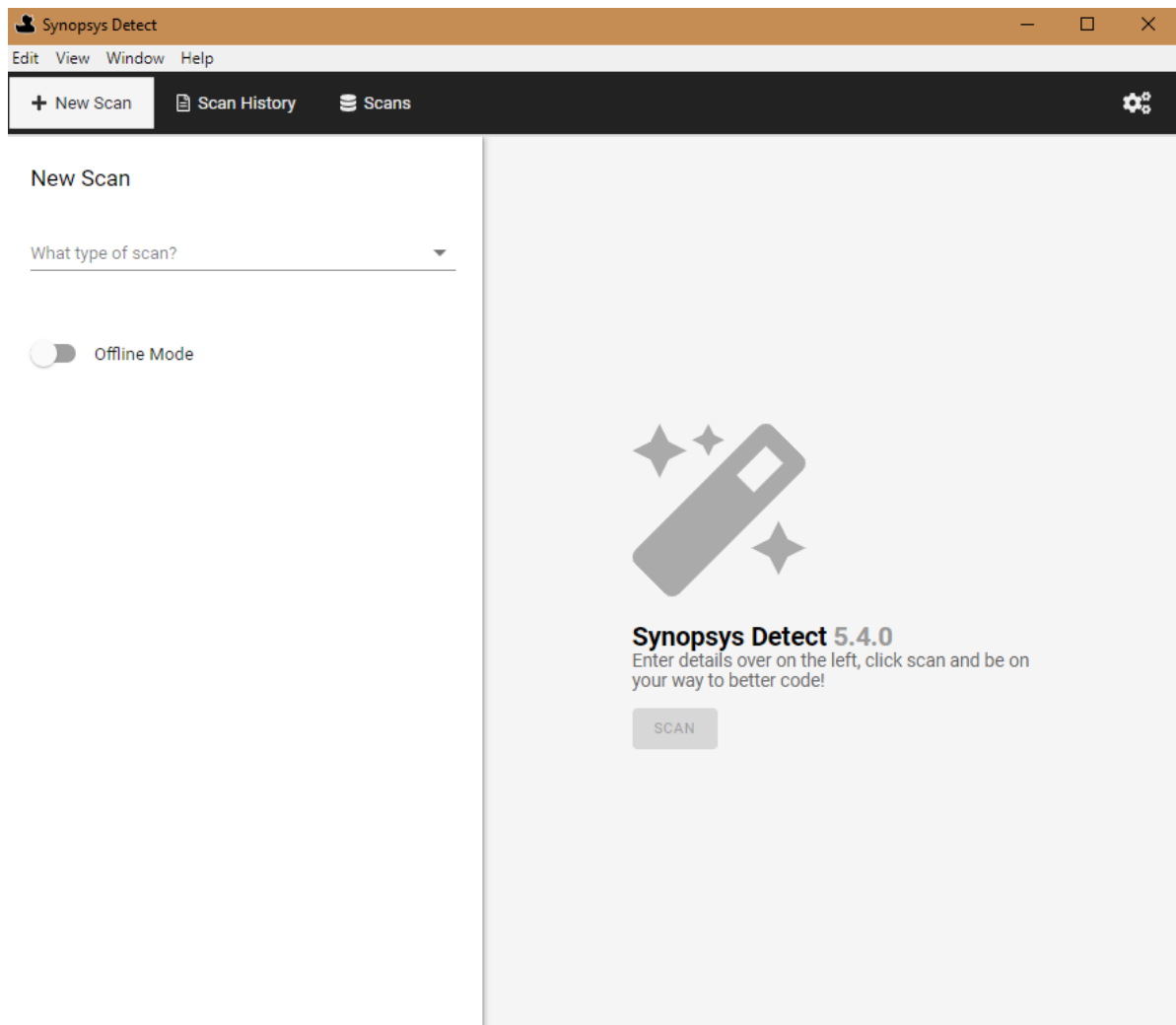
Creating a scan file

You can use Synopsys Detect (Desktop) to output the scan to a file which you can later upload to Black Duck by using Synopsys Detect (Desktop), as described below, the command line, or by using the Black Duck UI.

Note: Snippet scanning cannot be completed offline as it requires communication with the Black Duck server.

⚙️ To create a scan file:

1. Click **New Scan**.



2. Select the type of scan (**Source Directory**, **Binary/Executable**, or **Docker**).
3. Optionally, modify or configure any project or, for source directory scanning, scan settings by clicking **ADD** and selecting the setting.
4. Select **Offline Mode**.
5. Click **Scan**.

The status of the scan appears along with an option to cancel the scan.

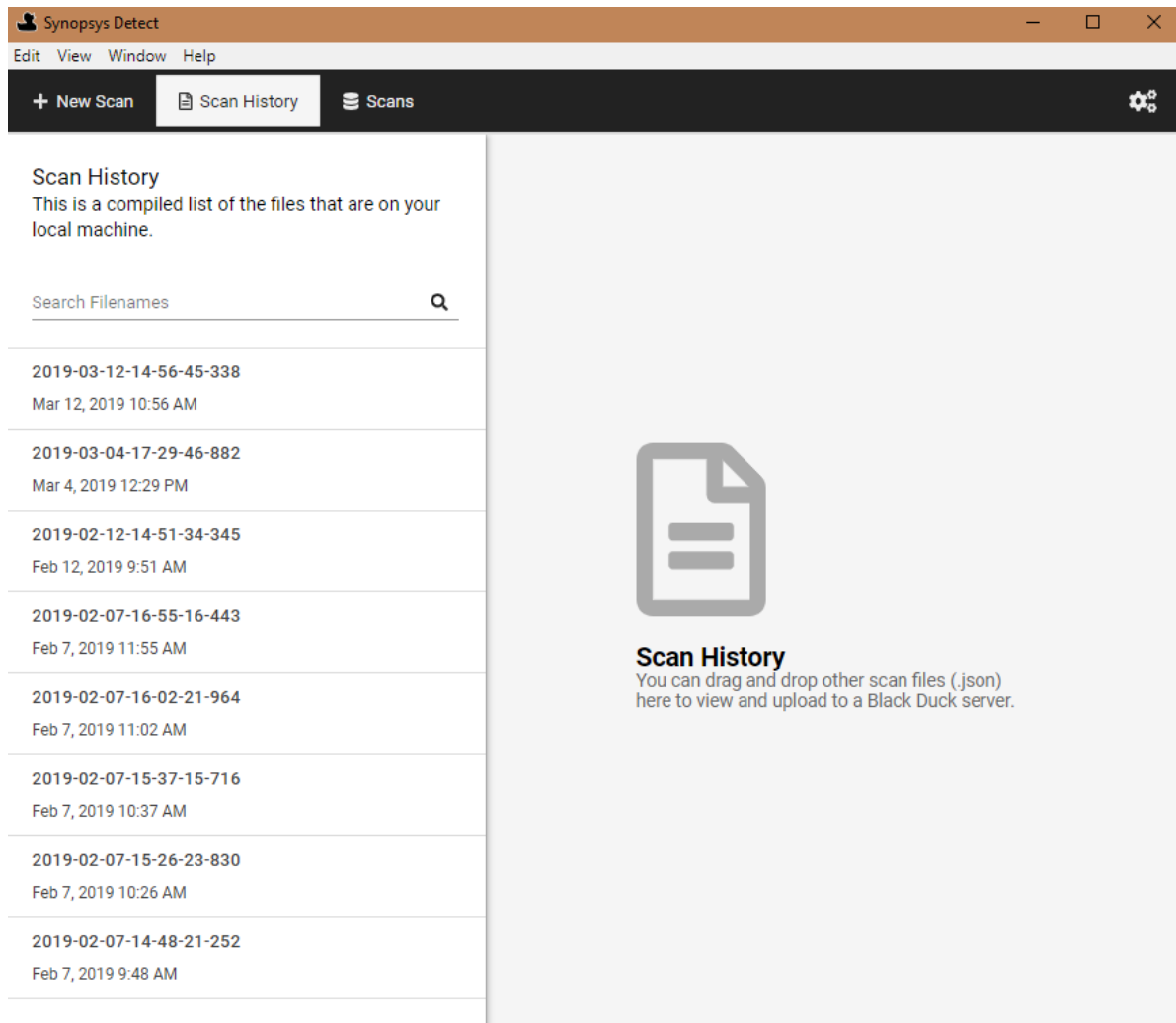
6. When the scan is complete, select the **Scan History** tab to view information on the completed scan.

Managing scans

Use the **Scan History** tab to manage your scans.

1. Click **Scan History**.

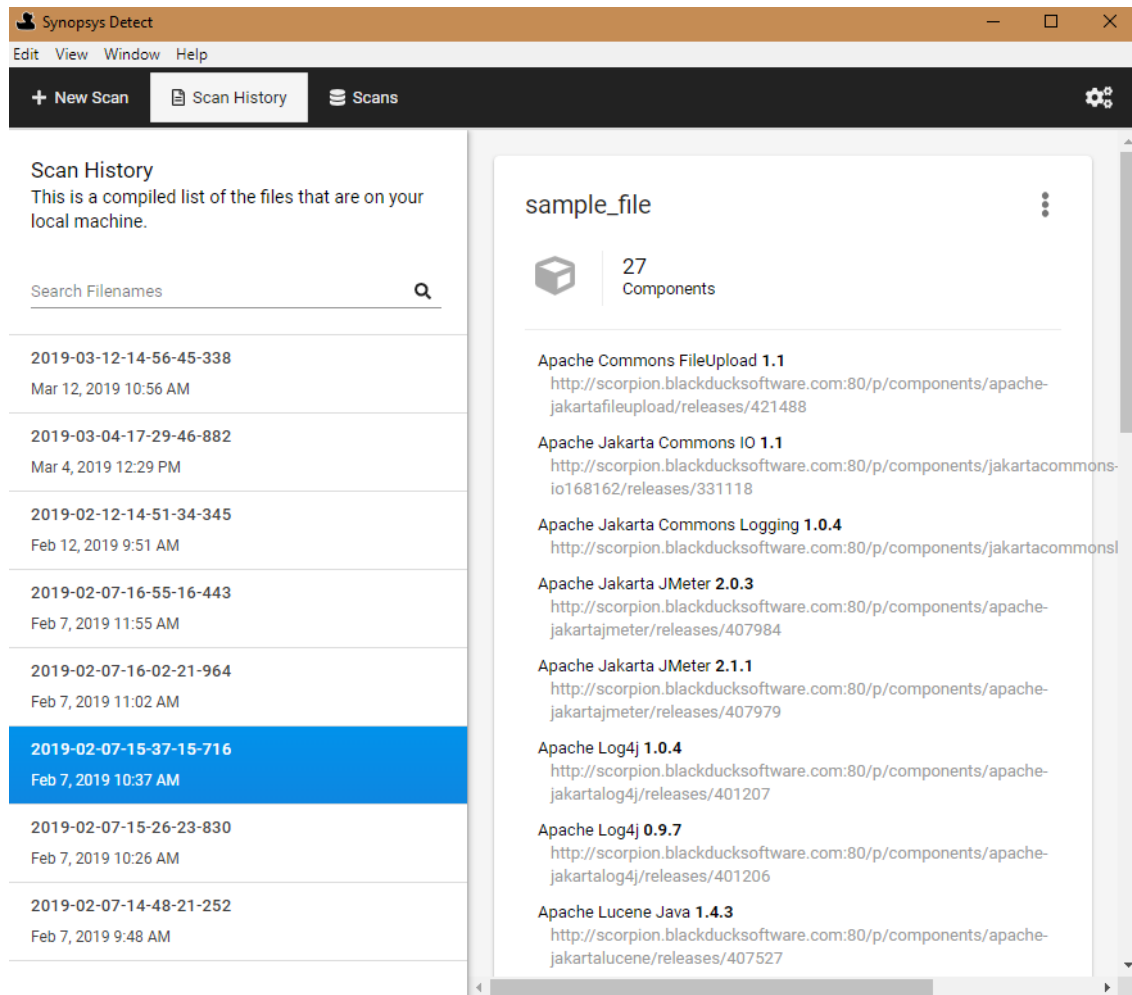
A list of scans on your local system appears in the left column of the tab.




Drag and drop scans from your local machine to this tab to manage them.

From this tab, select a scan and:

- View information on the contents of the scan:

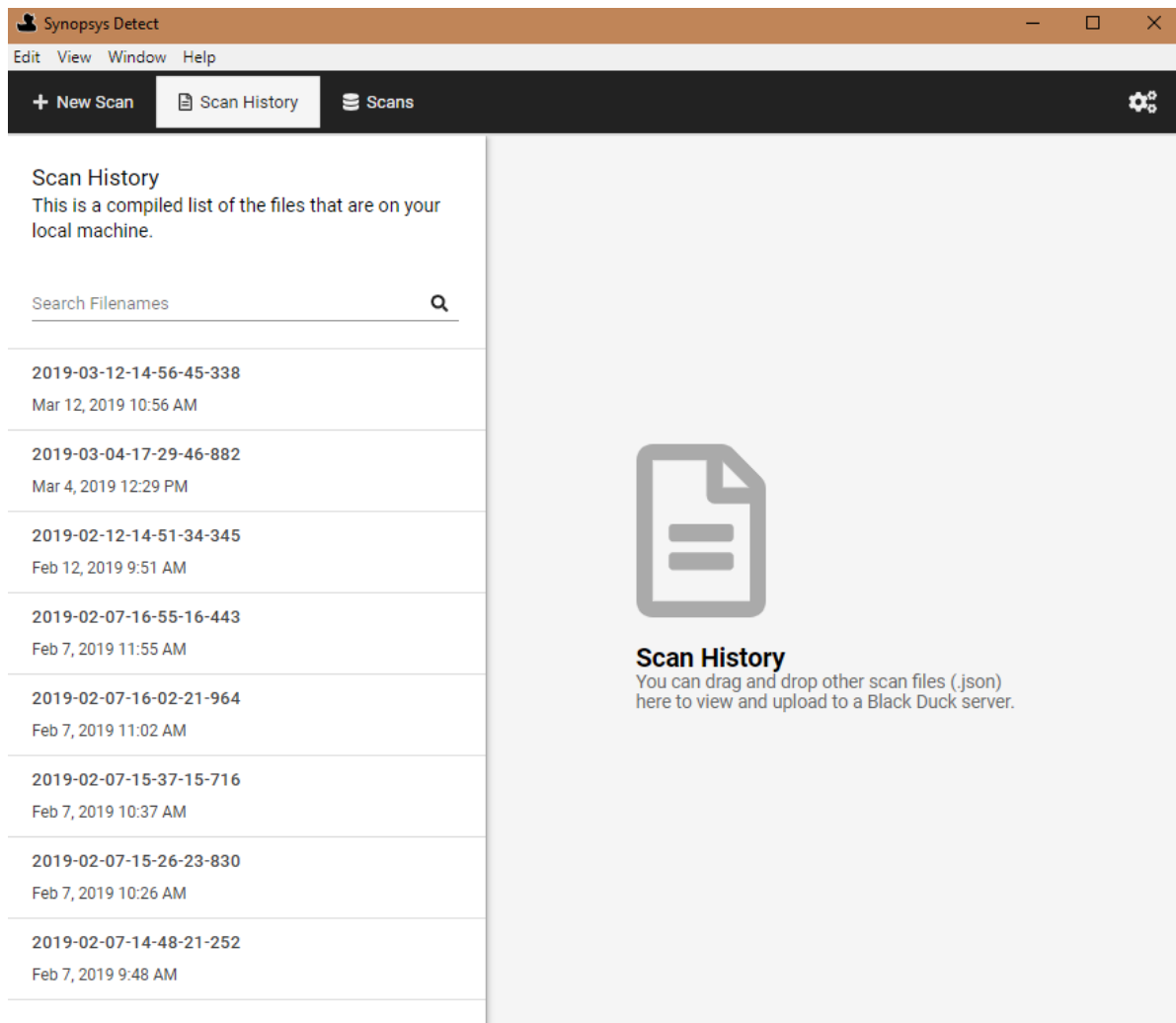



- View the location of the file on your system by clicking  and selecting **Show File**.
- Upload the file, as described in the next section.
- Delete the scan by hovering over the scan name in the left column and clicking **Delete**. Click **Yes** to confirm.

Uploading scan files to Black Duck

You can use Synopsys Detect (Desktop) to upload scan files to Black Duck.

1. Click **Scan History**.

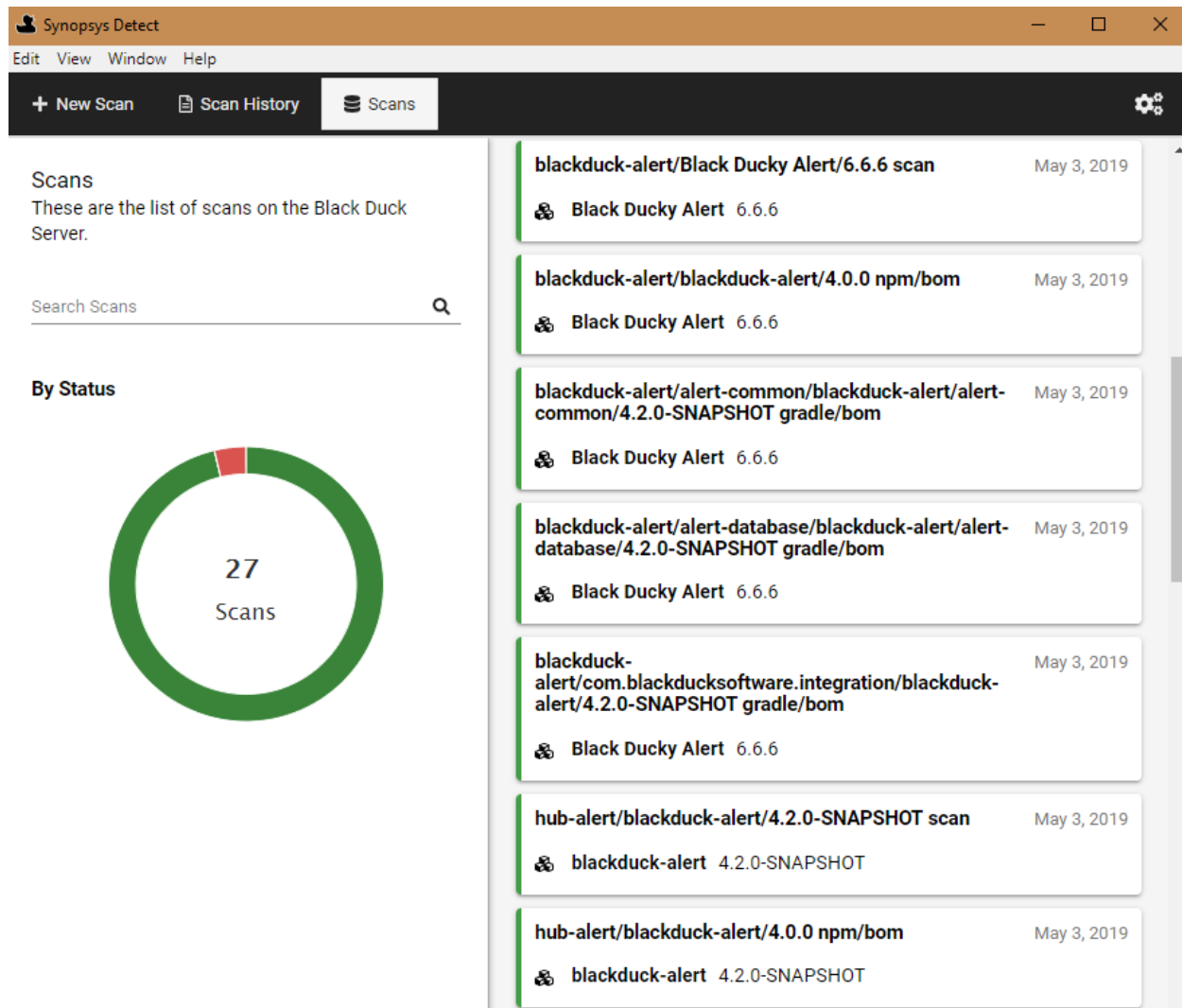


2. If the file is on your local system, you can drag and drop the scan file from your local machine to the **Scan History** tab.
3. Select the file to upload and click  in the upper right corner to display the file options.
4. Click **Upload Scan File to Black Duck**. The Upload Progress window appears showing you the status of the upload. Close the window when the process is complete.

You can confirm that the scan has been uploaded by clicking **Scans** and viewing the uploaded file.

Viewing uploaded scans

You can view the scans that have been uploaded to Black Duck's UI by clicking **Scans**:



This tab displays the following information:

- The left side of the tab shows uploaded scans by status (in progress, completed, or error).
Use the search field to find a scan or limit the scans shown.
- The right side of the page lists the scans and shows the following information for each scan:
 - Name
 - Project and project version scan is mapped to or indicates that the scan is not mapped to a project.
 - Date the scan was uploaded to Black Duck.

Select a scan to open the *Scan Name* page in Black Duck for the selected scan.

Note: The number of scanned bytes displayed in Synopsys Detect (Desktop) may differ from the number of scanned bytes shown in Black Duck. This is because of how Black Duck calculates and counts the number of bytes used. This is normal and is expected to occur in some scans.

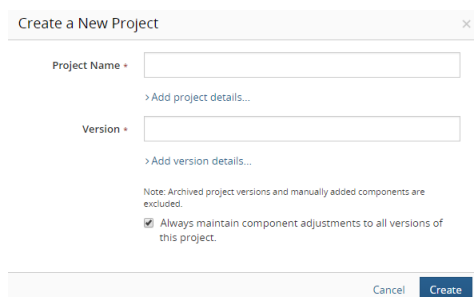
Creating a project

A project is the base unit in Black Duck. A project can be both a stand-alone development project and part of another project. For example, Apache Tomcat is a project in its own right but it may also be part of other, larger projects. You must create the projects that you want to make available for search by other developers in your organization.

Note that a project or application is limited to 10GB of Managed Code base.

⚙️ To create a project

1. Log in to Black Duck.
2. Click **+ Create Project** at the top of any page.



3. In the Create a New Project dialog box, enter a project name. This name must be unique among projects in Black Duck, although it can have the same name as a project in the Black Duck KB.

Tip: As a best practice, you should think about how other users will search for your projects when creating project names. For example, if your project is related to 3D graphics, naming it "3DGraphics" means that the user must type the entire project name in order to find your project. If you use a space or an underscore in the name, for example, "3D Graphics" or "3D_Graphics", the additional separator characters will allow users to locate the project using the search term "3D".

4. Optionally, select **Add project details** to enter additional information such as:
 - Description.

Tip: As a best practice, you should think about how other users will search for your projects when creating project descriptions. The description should be specific about what the project does and how it is unique, so that it is easily distinguishable from other similar projects.

- Name of the project owner in the **Owner** field.

Note: If the user you add is not already a project member, Black Duck adds the user to the project team.

By default, the user creating the project is the project owner. The owner has the ability to assign their projects to users and groups.

- Select a tier.¹

Note: To assign an application ID to a project, create the project, as described here, and then modify the project settings.

5. Type the version for this project in the **Version** field.
6. Optionally, select **Add version details** to enter additional information such as the planned release date, the project phase, and the method in which the project is being delivered.
7. By default, edits to a version of this project apply to all versions of this project, excluding archived versions and manually added components. Clear this option if you want edits to apply to specific versions only.
8. Click **Create**.

Black Duck displays the *Project Name* page.

Black Duck Projects
DP Sample Project

Project Versions: 1

Overview Settings

Create Version Filter versions... Add Filter

| Version | Phase | Last Updated | License | Security Risk | License Risk | Operational Risk |
|---------|-------------|--------------|-----------------|---------------|--------------|------------------|
| 2.0 | In Planning | Oct 22, 2018 | Unknown License | | | |

Displaying 1-1 of 1

Description
No description.

Created
Sep 4, 2018 by sysadmin

Updated
Sep 4, 2018 by sysadmin

Tags
No Tags

Mapping a scan to a project

Mapping a scan adds the scan data to the BOM of a project version.



Note: You can scan a Docker image or file directory location or archive more than once, but you only have to map it to a project version once. As long as the host and path used to uniquely identify the scanned location or image does not change, Black Duck automatically updates the BOM of the project with any new information discovered during subsequent scans.

⚙️ To map a scan to a project


1. Log in to Black Duck.


2. Click .

¹A tier lets you categorize projects in terms of importance to your company. Tier 0 projects are defined as those that are most critical to the company, where Tier 5 projects are defined as least critical.

| Scans 394.7 MB / ∞ Unlimited | | | | | |
|--|--------|--|-----------|---|------------------------|
|  Upload Scans | |  Delete | | Filter scans... Add Filter | |
| <input type="checkbox"/> | Status | Name | Scan Size | Last Updated | Mapped to |
| <input checked="" type="checkbox"/> | ✓ | pc_1210_2 | 1.2 MB | Dec 10, 2019 | pc_1210_2 |
| <input checked="" type="checkbox"/> | ✓ | pc_1210 | 1.2 MB | Dec 10, 2019 | pc_1210_1 |
| <input checked="" type="checkbox"/> | ✓ | hh nodegoat demo 3.0-3 scan | 17.1 MB | Dec 5, 2019 | hh nodegoat demo 3.0-3 |
| <input checked="" type="checkbox"/> | ✓ | hh nodegoat demo 3.0-3 npm/bom | | Dec 5, 2019 | hh nodegoat demo 3.0-3 |
| <input checked="" type="checkbox"/> | ✓ | hh ng dm 3.0-2 scan | 17.1 MB | Dec 5, 2019 | hh nodegoat demo 3.0-2 |
| <input checked="" type="checkbox"/> | ✓ | hh ng dm 3.0-2 npm/bom | | Dec 5, 2019 | hh nodegoat demo 3.0-2 |
| <input checked="" type="checkbox"/> | ✓ | MapScanToProjectActivityScan-190516-1651-17r67p6 | 566.2 KB | Dec 4, 2019 | test123 1.0 |

3. Do one of the following:

- Click  and select **Map to Project** in the row of the scan that you want to map.
- Select the path of the scan you want to map to open the *Scan Name* page.


Scans

ComplexBomMainProject_2015-12-04 10:28:23

Scan Details - for the last completed scan

| | | | |
|------------|--------------------------------|-------------|----|
| Path | / | Match Count | 74 |
| Host | scorpion.blackducksoftware.com | Folders | 22 |
| Created on | Mon, Aug 15, 2016 6:06 PM | Files | 73 |
| Scan Size | 1.19 MB | | |

Delete Scan

Map Scan to Project Version

This scan is not mapped to any versions.

+ Create Project

Project

start typing to select project...

Version

① Select a project to list its versions

Save

Scan History

| Status | Matches | Host | Path | Scan Size | Last Updated | Scan Initiated By | |
|----------|------------|--------------------------------|------|-----------|---------------------------|-------------------|-------------------------------------|
| Complete | 74 Matches | scorpion.blackducksoftware.com | / | 1.19 MB | Tue, Sep 29, 2020 1:17 PM | sysadmin | View BOM Import Log |

Displaying 1-1 of 1

4. Start typing the name of a project to progressively display matches in the **Project** field.

If necessary, select **Create Project** to create a new project and version.

5. Select the project version to which you want to map the component scan.

If necessary, select **Create Version** to create a new version for a project.

6. Click **Save**.

Black Duck displays the name and version of the project to which you mapped the component scan. Select the link to open the BOM page.

Note: Black Duck displays an aggregate project version BOM. If a component version appears more than once in an archive, it is only displayed in the BOM once.

Chapter 3: Viewing risk in Black Duck

Black Duck helps you understand the type and severity of risks, at several levels of detail, across your projects. The data used to calculate risk is provided by the Black Duck KB.

Use the following pages to identify and manage risk in projects:

- Dashboard pages
- Project version page/**Components** tab
- Project version page/**Security** tab

Note that the security risk values shown use CVSS v2 or CVSS v3.x scores, depending on which security risk calculation you selected; by default, CVSS v2 scores are shown. Note that the security risk graph displays a Critical risk category with a value of 0, if you selected CVSS v2.

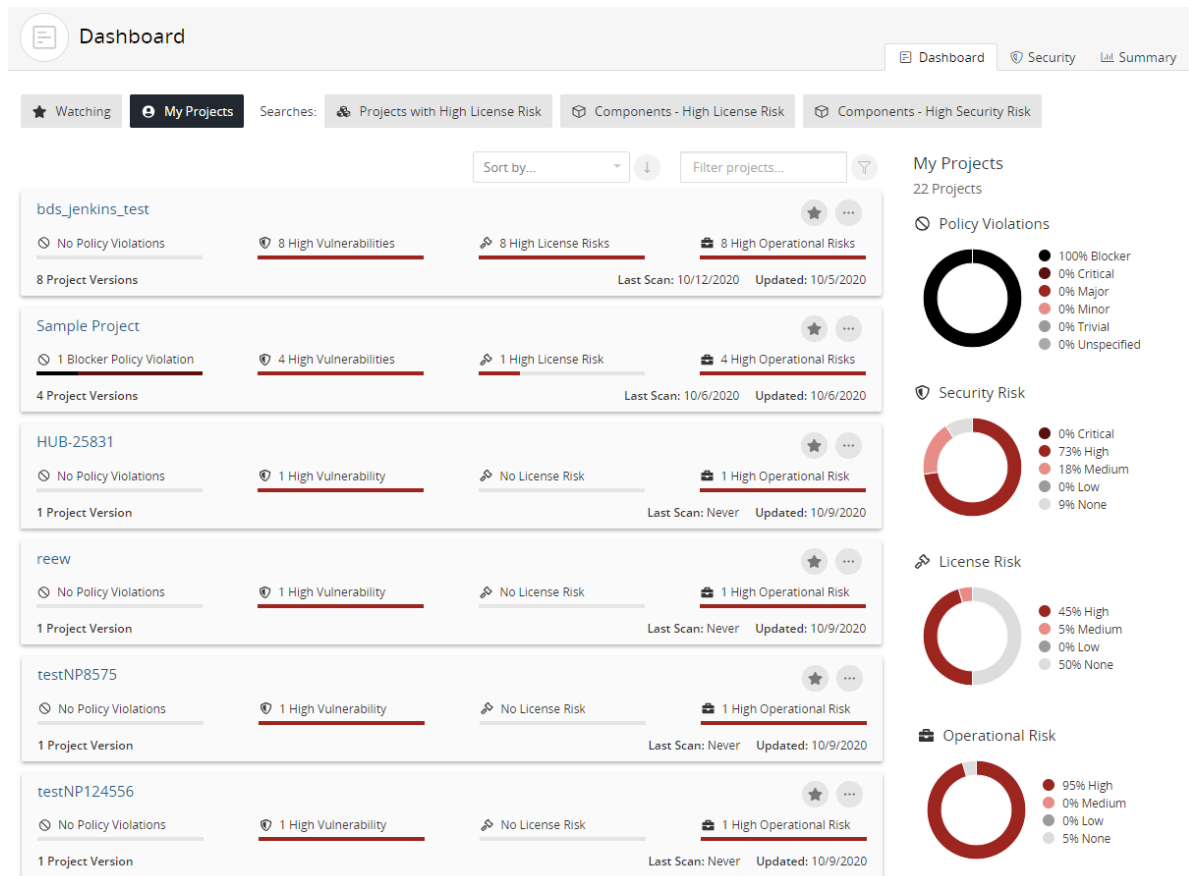
Dashboards

Dashboards provide a high-level overview of risk from different perspectives.

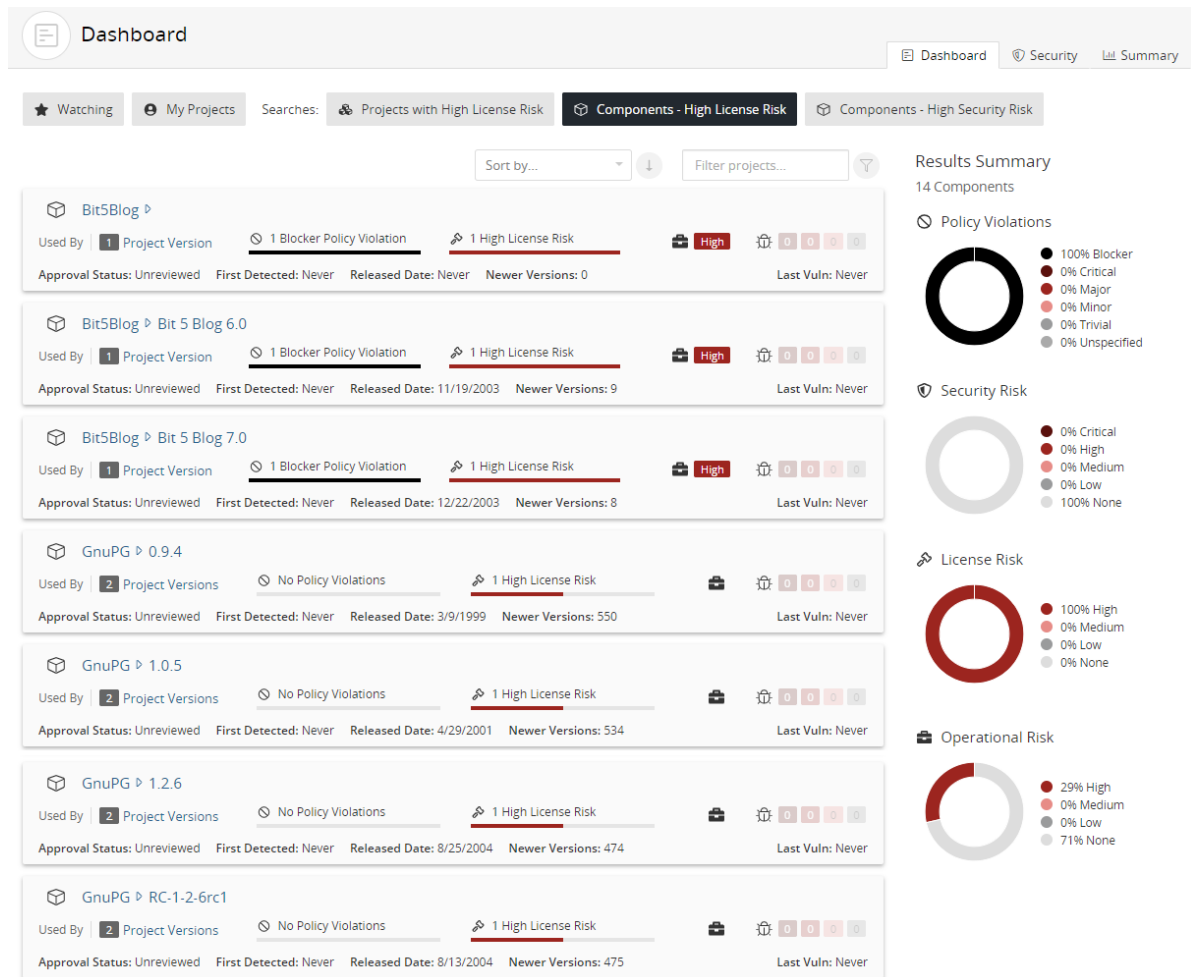
Note: Dashboards will not contain any project or component information until you create projects and then map scans to these projects or manually add components to BOMs. The risk information for the components in your project versions' BOMs will then appear on the Dashboard pages.

- Use the Dashboard to view the overall risk across all projects.

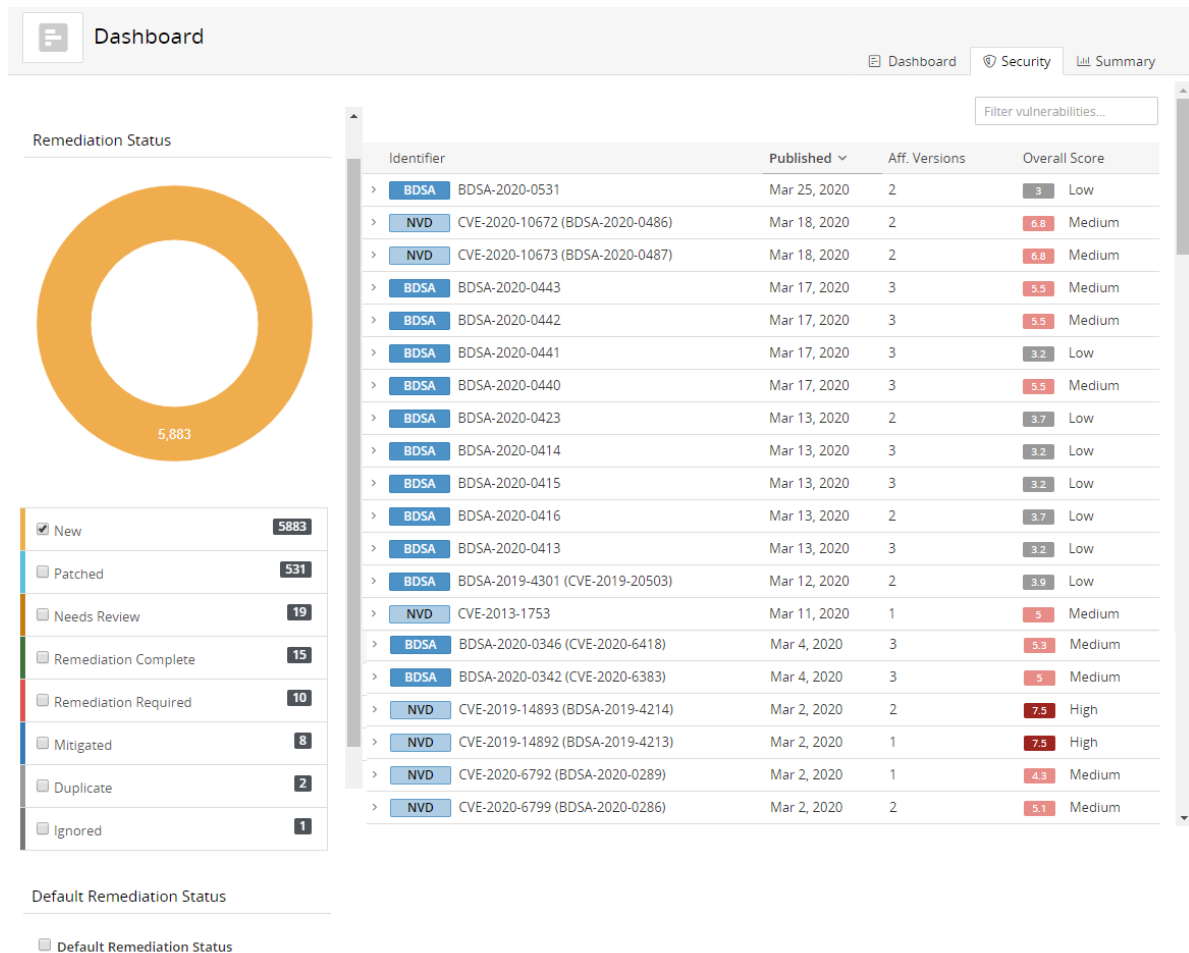
You can view the projects that interest you by using the **Watching** or **My Projects** dashboard or create a custom dashboard by saving your project search results.



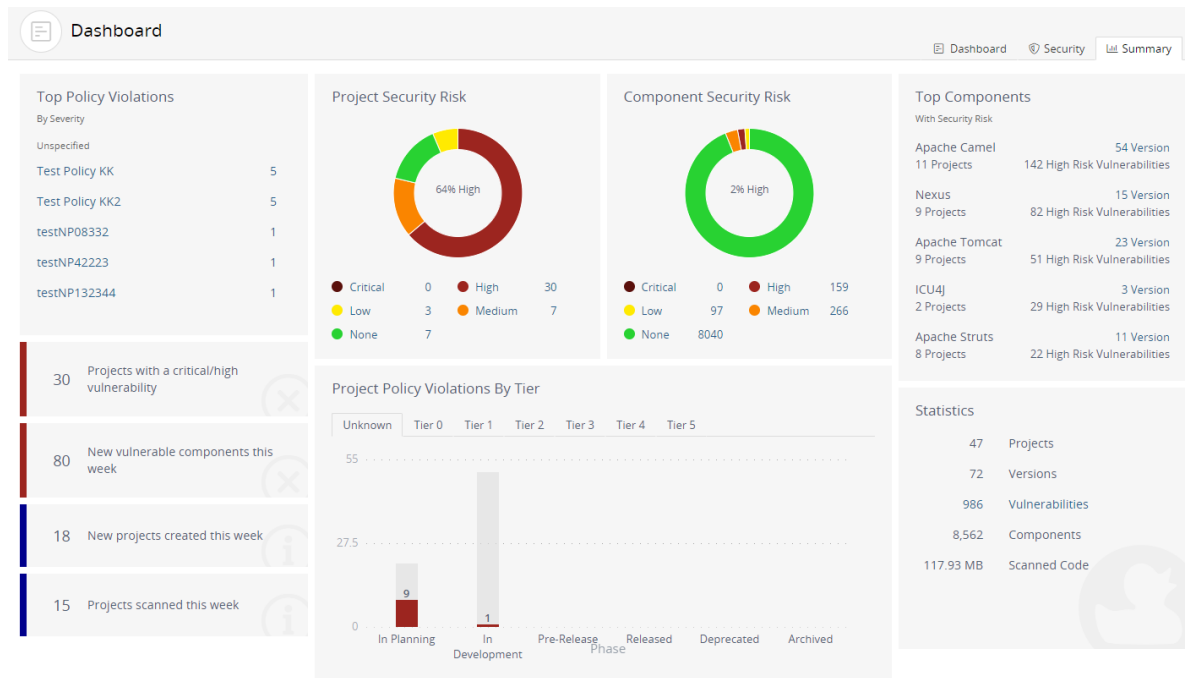
Create a saved component search to view the components that interest you that are used in one or more projects.



- Use the Security Dashboard to view the security risk associated with all the vulnerabilities that exist in your projects. This dashboard also shows the remediation status of all the vulnerabilities that exist within the projects.



- Use the Summary Dashboard to view the overall health of the projects you have permission to view and identify areas of concern.



Note:

- The Dashboard page that appears when you log in depends on the last main dashboard (Dashboard, Components, Security, or Summary) you viewed prior to previously logging out.



- Click **Dashboard** to view the last dashboard you viewed.
- Click the logo in the upper left corner of the navigation bar to view the **My Projects** dashboard.

Project version pages

- Use the project version page/**Components** tab, also known as the project version BOM, to view the components, specific to that project version, that have security, license, and operational risk.

Black Duck Projects
Sample Project • 1.0

Navigation: Project | Versions: 1 | Phase: In Planning | Distribution: External | Scan Status: Up to Date | Components | Security | Source | Reports | Details | Legal | Settings

Security Risk
Number of Components

| | |
|----------|----|
| Critical | 2 |
| High | 2 |
| Medium | 0 |
| Low | 0 |
| None | 10 |

License Risk
Number of Components

| | |
|--------|---|
| High | 0 |
| Medium | 1 |
| Low | 0 |
| None | 7 |

Operational Risk
Number of Components

| | |
|--------|----|
| High | 10 |
| Medium | 0 |
| Low | 0 |
| None | 4 |

Buttons: Add, Compare to..., Print..., Select all, Bulk Actions, Filter components..., Add Filter

| Component | Source | Match Type | Usage | License | Security Risk | Operational Risk | Actions |
|-------------------------------|---------|-------------------|--------------------|------------|-------------------------|------------------|----------------|
| Apache Commons FileUpload 1.1 | 1 Match | Direct Dependency | Dynamically Linked | Apache-2.0 | 1 High, 1 Medium, 1 Low | High | Info, Download |
| Apache log4j 0.9.7 | 1 Match | Direct Dependency | Dynamically Linked | Apache-2.0 | 0 | High | Info, Download |
| Apache log4j 1.0.4 | 1 Match | Direct Dependency | Dynamically Linked | Apache-1.1 | 1 High | High | Info, Download |
| Apache Lucene 1.4.3 | 1 Match | Direct Dependency | Dynamically Linked | Apache-2.0 | 0 | High | Info, Download |
| Apache-Jakarta Jmeter 2.0.3 | 1 Match | Direct Dependency | Dynamically Linked | Apache-2.0 | 3 High | High | Info, Download |
| Apache-Jakarta Jmeter 2.1.1 | 1 Match | Direct Dependency | Dynamically Linked | Apache-2.0 | 3 High | High | Info, Download |
| BitSBlog Bit 5 Blog 6.0 | 1 Match | Direct Dependency | Dynamically Linked | GPL-2.0+ | 0 | High | Info, Download |

- Use the project version page/ **Security** tab to view the security vulnerabilities of each severity associated with the components used in a project version.

Black Duck Projects
bds_jenkins_test • 2020_03_29--19_25_24

Project | Phase: In Development | Components: Up to Date | Scans: Up to Date

Components | Security | Source | Reports | Details | Settings

Security Risk
Number of Unique Component Origins

Critical 0 High 2 Medium 15 Low 8

Filter components... Add Filter

Hibernate Validator 5.2.4.Final
maven: org.hibernate:hibernate-validator:5.2.4.Final
Vulnerabilities 1

iText, a JAVA-PDF library 5.3.2
maven: com.itextpdf:itextpdf:5.3.2
Vulnerabilities 1

Jersey 1.13
maven: com.sun.jersey:jersey-core:1.13
Vulnerabilities 1

Jersey 1.13
maven: com.sun.jersey:jersey-client:1.13
Vulnerabilities 1

Jetty: Java based HTTP/1.x, HTTP/2, Servlet, WebSocket Server 7.1.0.v20100505
maven: org.eclipse.jetty:jetty-http:7.1.0.v20100505
Vulnerabilities 0

Jetty: Java based HTTP/1.x, HTTP/2, Servlet, WebSocket Server 7.1.0.v20100505
maven: org.eclipse.jetty:jetty-util:7.1.0.v20100505
Vulnerabilities 0

Hibernate Validator 5.2.4.Final
maven: org.hibernate:hibernate-validator:5.2.4.Final
2 Known Vulnerability

Short Term Upgrade Recommendation
5.4.3.Final
Vulnerabilities

Long Term Upgrade Recommendation
6.1.2.Final
Has no known vulnerabilities

| Identifier | Published | Overall Score | Status | CWE | Exploit | Workaround | Solution |
|-------------------|--------------|---------------|--------|---------|---------|------------|----------|
| BDSA-2019-3481 | Nov 13, 2019 | 3.2 Low | New | CWE-79 | - | ✓ | ✓ |
| NVD CVE-2017-7536 | Jan 10, 2018 | 4.4 Medium | New | CWE-470 | - | - | - |

Displaying 1-2 of 2

Capture screenshot

Viewing your dashboards

Use dashboards to 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 your projects and components used in your projects.

So that you can view the projects and project versions that are important to you, Black Duck's provides two 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 Dashboard page at the project level.

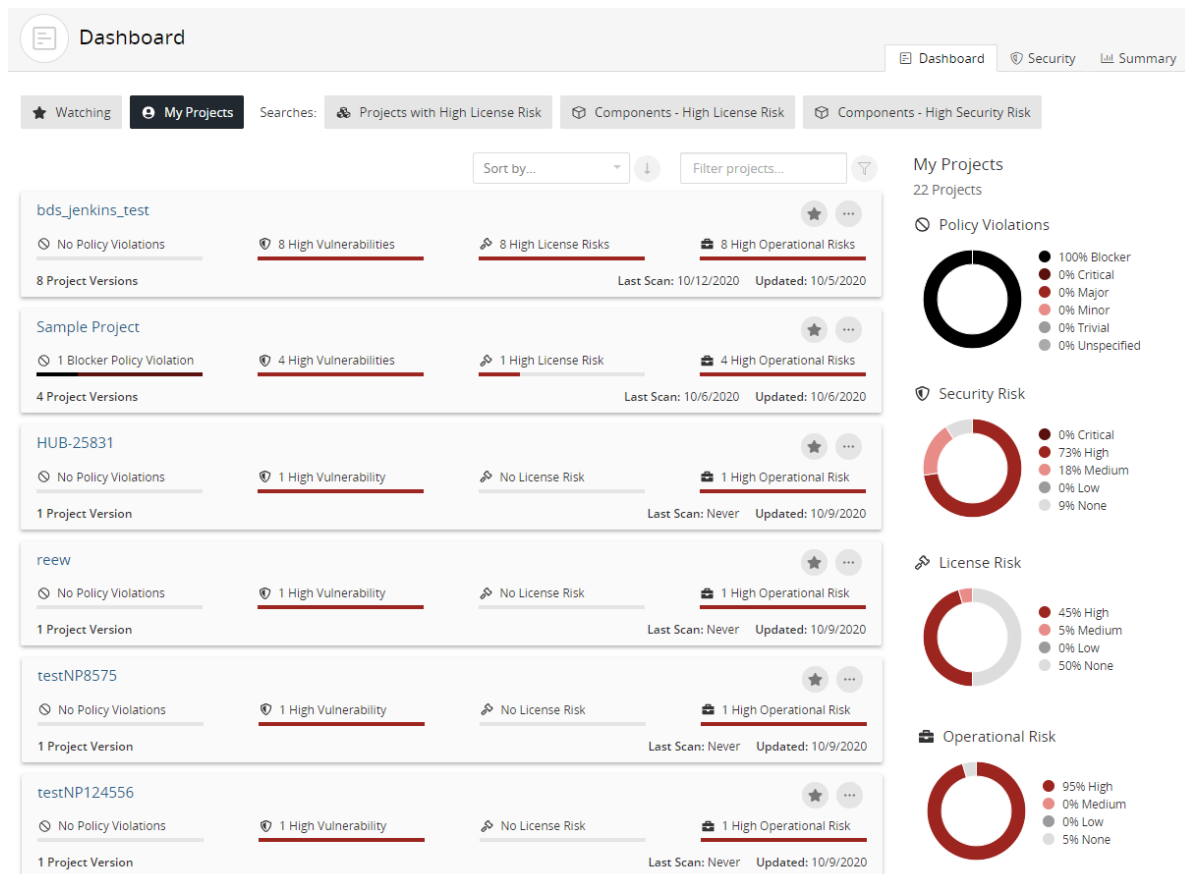
In addition, you can create custom dashboards so that you can quickly view the project versions or component versions that are important to you: search for projects, search for components, save the searches and then use this page to view dashboards from those saved searches. Dashboards based on saved searches display information at the project version or component version level.

Viewing dashboards

- ⚙️ To view the dashboards

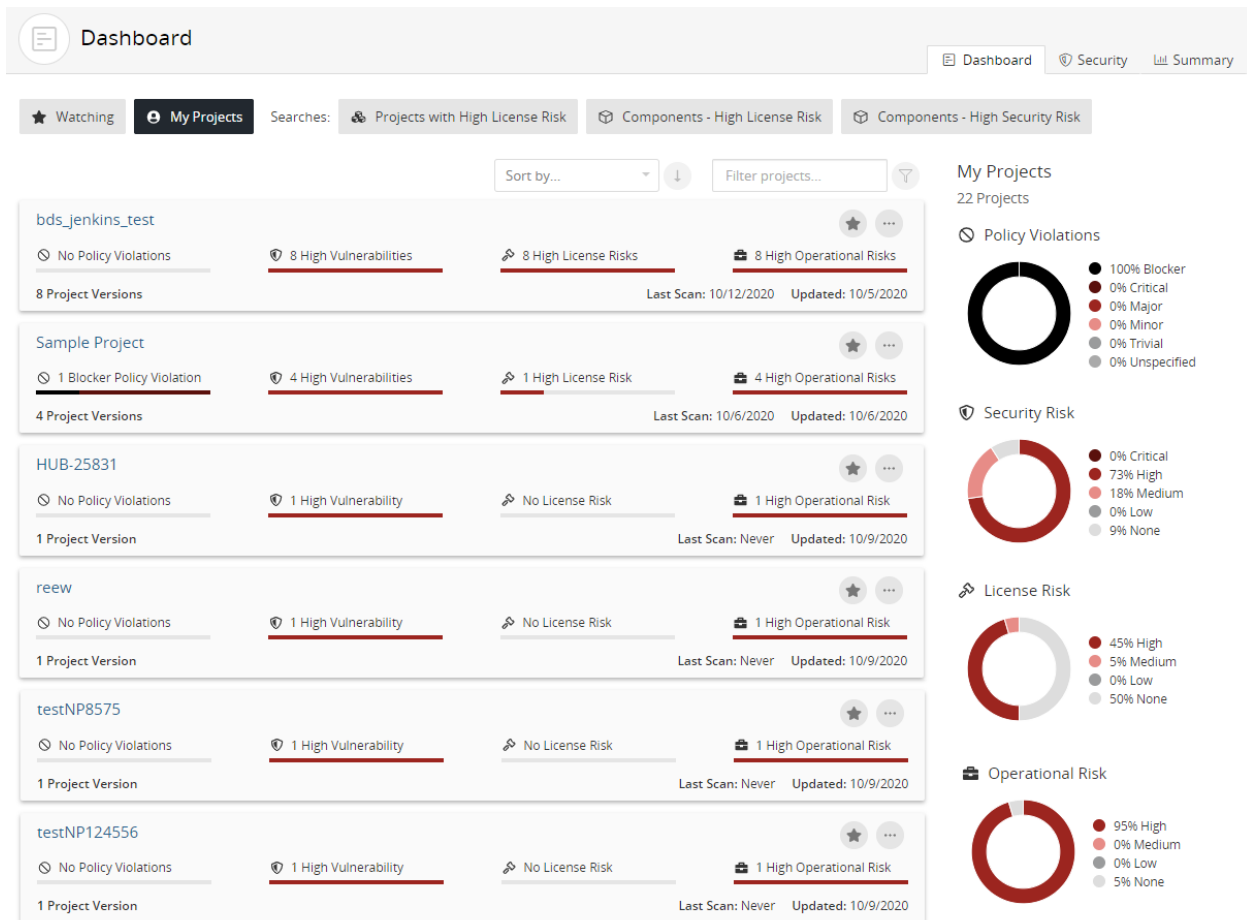
1. Click  to display the dashboards.

The dashboard page that appears depends on the last main dashboard you viewed prior to previously logging out. If not displayed, select **Dashboard** to display your dashboards.

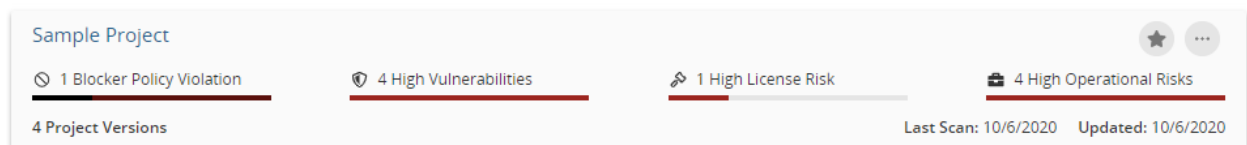


About the Watching and My Projects dashboards

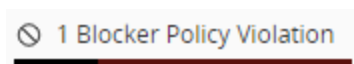
Use the **Watching** or **My Projects** dashboards to view risk and policy violation information at the *project* level.



The following information is shown for each project:



- To view policy violation information for a specific project:
 - Use the bar to view the number of project versions with the highest policy severity level.



Note: The text states the number of project versions with this highest policy severity level, not all policy severity levels affecting this project.

- Hover over the bar to see the number of project versions with their highest severity level of policy violations:

Policy Violations

by Project Version

| | | | |
|----------|----------|---|-------------|
| 1 | Blocker | 0 | Minor |
| 3 | Critical | 0 | Trivial |
| 0 | Major | 0 | Unspecified |

* Each project version is counted once by its highest severity risk

In the above example, there are four project versions which have policy violations; one version has a policy violation which has Blocker as the highest severity level, the other three have policy violations have Major as the highest severity level. Note that this does not indicate the number of policy violations in these versions, just the highest severity level for each version.

■ To view risk information:

- Use the risk bar to view the number of project versions with the highest risk level:

Security risk:


 4 High Vulnerabilities

License risk:


 1 High License Risk

Operational risk:


 4 High Operational Risks

Note: The text states the number of project versions with this highest risk level, not all risk levels affecting the versions.

- Hover over a risk bar to see the number of versions of this project with their highest level of risk.

Security Risk

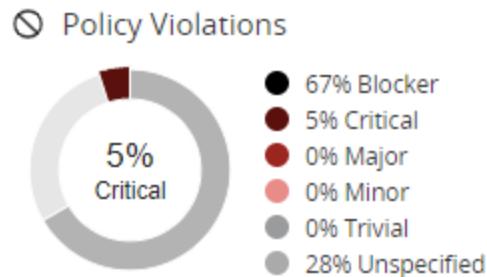
by Project Version

| | | | |
|----------|----------|---|--------|
| 0 | Critical | 0 | Medium |
| 4 | High | 0 | Low |

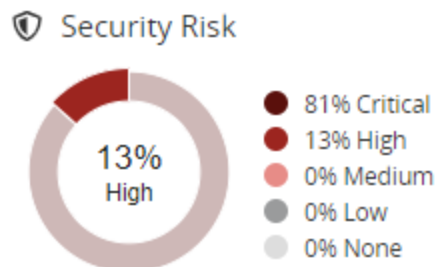
* Each project version is counted once by its highest severity risk



If a project version has risk, the version is only counted once and only its highest risk level is shown.

- Use the graphs to see overview information for all projects in this dashboard.
 - The risk graph shows the percentage of projects in this dashboard that have policy violations by severity level. You can also hover over an area in the graph to view this information:



- The risk graphs show the percentage of projects in this dashboard that have this level of security, license, or operational risk. You can also hover over an area in the graph to view this information:

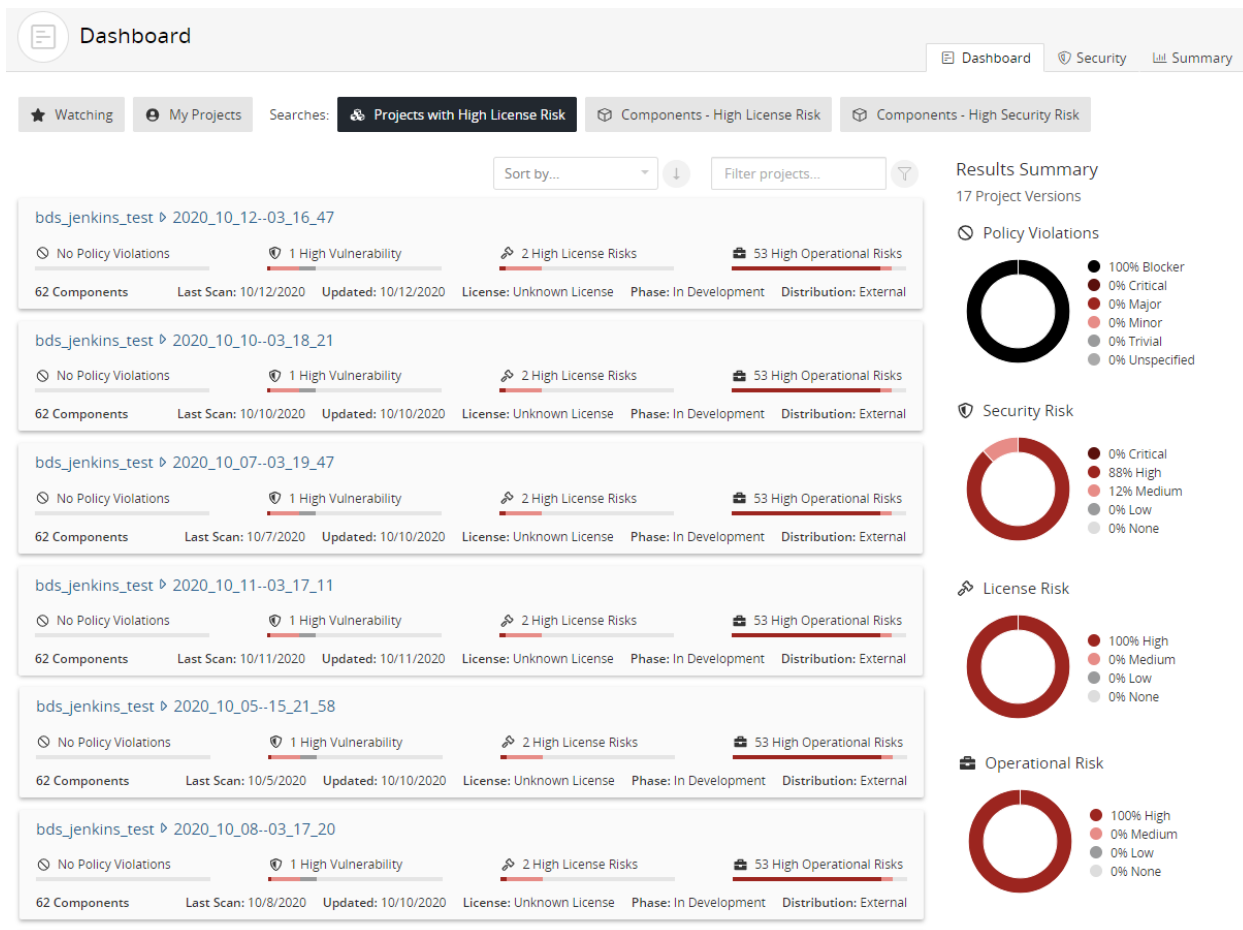


- Hover over a value in the legend to highlight the value in the graph.
- View additional information for each project, including:
 - Number of versions.
 - Last scan date.
 - Date when this project was last updated, such as when a scan that was mapped to any project version was last run or when the BOM for any project version was last updated, either manually or by a new scan.
- Select a project name to view the *Project Name* page which lists all versions of this project.
- Manage how the projects are shown in these dashboards:
 - Use the **Sort by** field to select an attribute to sort by and click an arrow to select the sort order (ascending) or (descending).
 - Use the **Filter projects** field to filter the projects shown in either dashboard.
- Use the icons   to [manage your watched projects](#) or [delete a project](#).

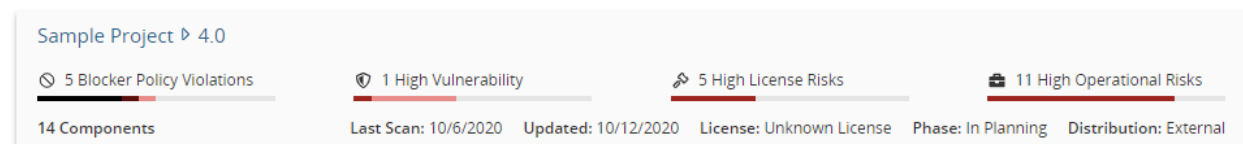
About saved searches dashboards


Use a saved search to view risk and policy violation information at the project version or component version level.

Project version saved searches



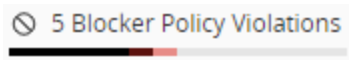
The following information is shown for each project version:



-  located in front of the saved search name indicates that this is a project saved search.
- To view policy violation information for a specific project version:
 - Use the bar to see the number of components with the highest policy severity level for this project version.

For example, the following shows that while there are components with lower severity levels, the highest policy severity level for this project version is Blocker and there are five components that

have Blocker as their highest policy severity level.



Note: The text states the number of components with the highest policy severity level for this project version, not all policy severity levels affecting this project version.

- Hover over the bar to see the number of components with policy violations by the highest policy severity level:

Policy Violations

by Component

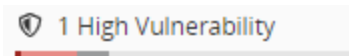
| | | | |
|---|----------|---|-------------|
| 5 | Blocker | 1 | Minor |
| 1 | Critical | 0 | Trivial |
| 0 | Major | 0 | Unspecified |

* Each component is counted once by its highest severity risk

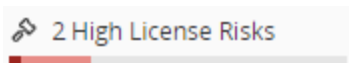
If a component has a policy violation, the component is only counted once and only its highest policy severity level is shown.

- To view risk information:
 - Use the risk bars to quickly view the number of components with the highest level of security, license, or operational risk.

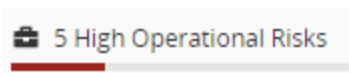
Security risk:



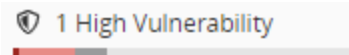
License risk:



Operational risk:



For example, the following shows that while there are components with lower risk, the highest security risk for this project version is High and that one component in this project version has a high level of security risk as their highest risk level:



- Hover over the bar to see the number of components for each risk category.

Security Risk by Component



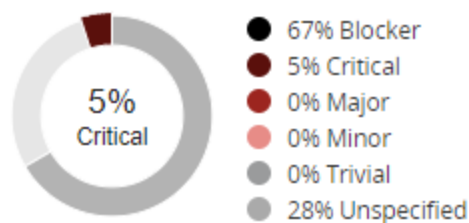
* Each component is counted once by its highest severity risk

In this example, there is one component that has a high risk level as its highest risk, 10 components that have medium risk as their highest risk level, and six components that have low risk as their highest risk level.

Note: Each component is only counted once and is shown with its highest risk level.

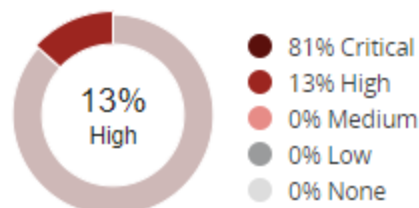
- Use the graphs to view overview information for all project versions in this dashboard categorized by policy severity and risk levels. The graphs lists the percentages for each level. You can also:
 - Hover over the graph to view the percentage of project versions with policy violations for each policy severity level.


Policy Violations



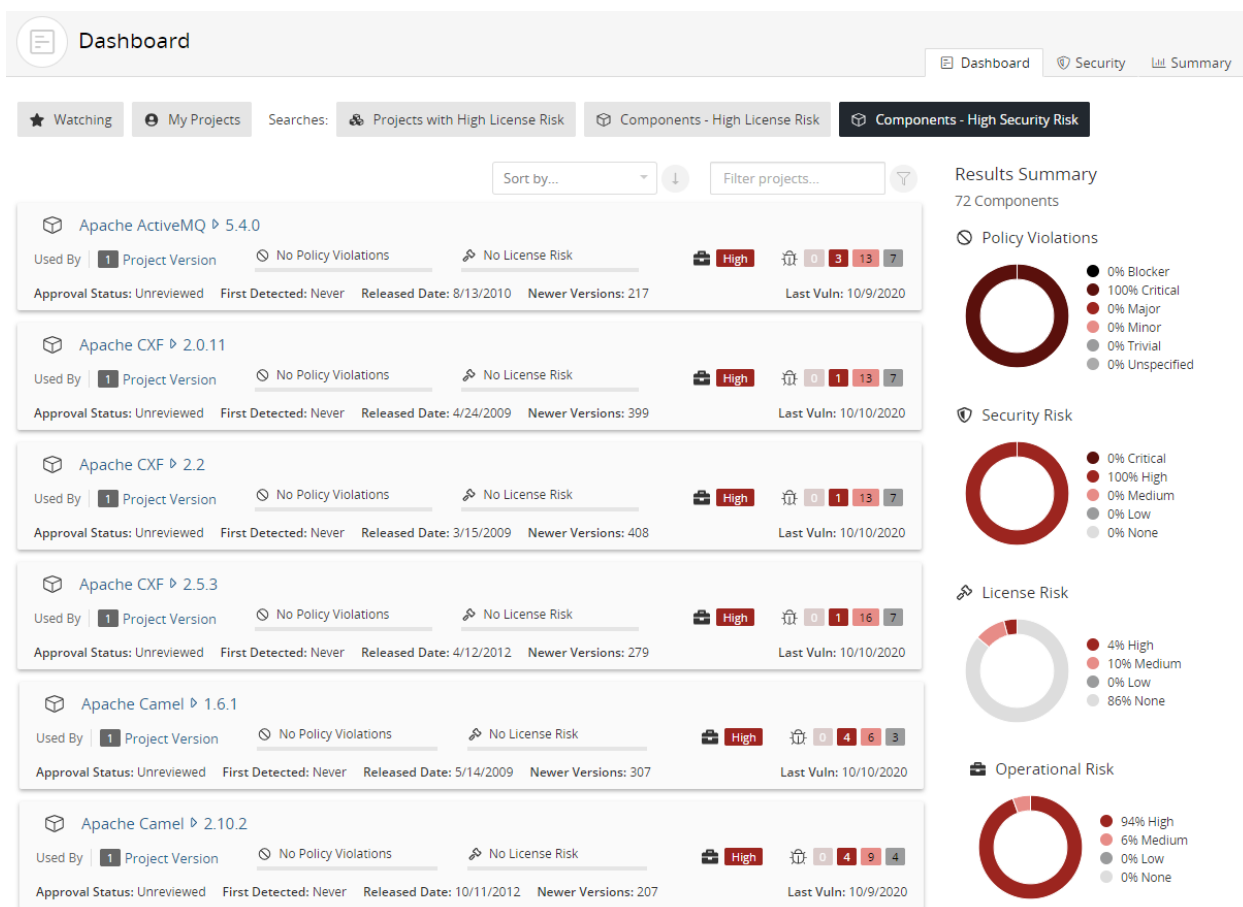
- Hover over the graph to view the percentage of project versions in this dashboard for each risk level.

Security Risk



- Hover over a value in the legend to highlight the value in the graph.
- For each project version, the dashboard also shows:
 - Number of components in this project version.
 - Last scan date.
 - Date when this project version was last updated, such as when a scan that was mapped to this project version was last run or when the BOM for this project version was last updated, either manually or by a new scan.
 - License of this project version.
 - Phase for this project version.
 - Distribution of this project version.
- Select the project or version name to view the BOM.
- Manage how the projects are shown in these dashboards:
 - Use the **Sort by** field to select an attribute to sort by and click an arrow to select the sort order (ascending) or  (descending).
 - Use the **Filter projects** field to filter the projects shown in the dashboard.

Component saved searches



The screenshot displays the Black Duck dashboard interface. At the top, there's a navigation bar with 'Dashboard', 'Security', and 'Summary' tabs. Below this, a 'Watching' section shows active searches: 'Projects with High License Risk', 'Components - High License Risk', and 'Components - High Security Risk'. The main content area lists several project versions with their respective risk metrics and status.

| Project Name | Version | Used By | Policy Violations | License Risk | Risk Level | High | Medium | Low | Trivial | Unspecified | Last Vuln |
|-----------------|---------|-------------------|----------------------|-----------------|------------|------|--------|-----|---------|-------------|------------|
| Apache ActiveMQ | 5.4.0 | 1 Project Version | No Policy Violations | No License Risk | High | 0 | 3 | 13 | 7 | | 10/9/2020 |
| Apache CXF | 2.0.11 | 1 Project Version | No Policy Violations | No License Risk | High | 0 | 1 | 13 | 7 | | 10/10/2020 |
| Apache CXF | 2.2 | 1 Project Version | No Policy Violations | No License Risk | High | 0 | 1 | 13 | 7 | | 10/10/2020 |
| Apache CXF | 2.5.3 | 1 Project Version | No Policy Violations | No License Risk | High | 0 | 1 | 16 | 7 | | 10/10/2020 |
| Apache Camel | 1.6.1 | 1 Project Version | No Policy Violations | No License Risk | High | 0 | 4 | 6 | 3 | | 10/10/2020 |
| Apache Camel | 2.10.2 | 1 Project Version | No Policy Violations | No License Risk | High | 0 | 4 | 9 | 4 | | 10/9/2020 |

On the right side, there are four donut charts summarizing the results:

- Results Summary:** 72 Components. Legend: 0% Blocker, 100% Critical, 0% Major, 0% Minor, 0% Trivial, 0% Unspecified.
- Policy Violations:** Legend: 0% Critical, 100% High, 0% Medium, 0% Low, 0% None.
- License Risk:** Legend: 4% High, 10% Medium, 0% Low, 86% None.
- Operational Risk:** Legend: 94% High, 6% Medium, 0% Low, 0% None.

The following information is shown for each component.

Apache Struts ▾ 2.3.7
 Used By | **9** Project Versions | 4 Critical Policy Violations | No License Risk | **High** | 0 3 28 11
 Approval Status: Unreviewed | First Detected: Never | Released Date: 11/6/2012 | Newer Versions: 80 | Last Vuln: 10/9/2020

- located in front of the saved search name indicates that this is a component saved search.
- Select the component name/version to display the [Component Name Version page](#).
- View the number of project versions that use this component version as shown by the value next to **Used By**.

Used By | **2** Project Versions

Select **Project Versions** to open the Where Used dialog box.

Used in ×


Apache Struts - 1.2.2 is being used in 1 Project Version

| Project Name | Phase | License | Review Status | Security Risk |
|--------------------------------------|-------------|--------------------|---------------|---------------|
| Sample Project - 4.0 | In Planning | Apache License 2.0 | Not Reviewed | 0 3 6 9 |

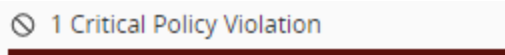
Close

This dialog box shows the project versions that use this version of the component.

| Column | Description |
|--------------|---|
| Project Name | Name of project and version that uses this component version. Select the project name to display the project version's Components tab. |
| Phase | Project Phase . |
| License | License for this component version. |

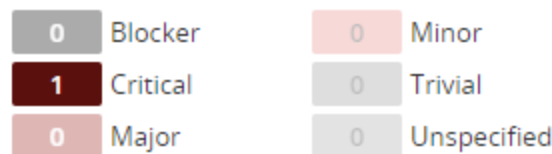
| Column | Description |
|---------------|---|
| Review Status | Whether this component has been reviewed in this project version. |
| Security Risk | <p>Lists the vulnerabilities for each severity level, from left to right: Critical, High, Medium, and Low.</p>  <p>Select a value to display the Security tab of the the Black Duck KB<i>Component Name Version</i> page, which lists the vulnerabilities associated with this version of this component.</p> |

- Use the bar to quickly see the number of components with the highest policy severity level.



Select the bar to see the number of components with policy violations by severity level:

Policy Violations by Component



* Each component is counted once by its highest severity risk

Note: A component is only counted once with the highest policy severity level, not all policy severity levels affecting this component.

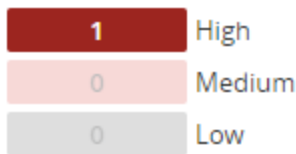
- Use the bar to quickly view the number of components with the highest level of license risk.



Select the bar to view the number of components in each risk category.

License Risk

by Component



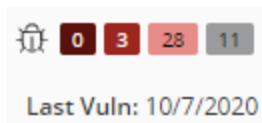
* Each component is counted once by its highest severity risk

- View the operational risk for this component version:



- View the number of vulnerabilities by severity associated with this component version for each severity level, from left to right: Critical, High, Medium, and Low.


The **Last Vuln** date is the date when a vulnerability for this component was last updated in Black Duck (by the Black Duck KnowledgeBase or a user).



Select a value to display the **Security** tab of the the Black Duck KBComponent Name Version page, which lists the vulnerabilities associated with this version of this component.

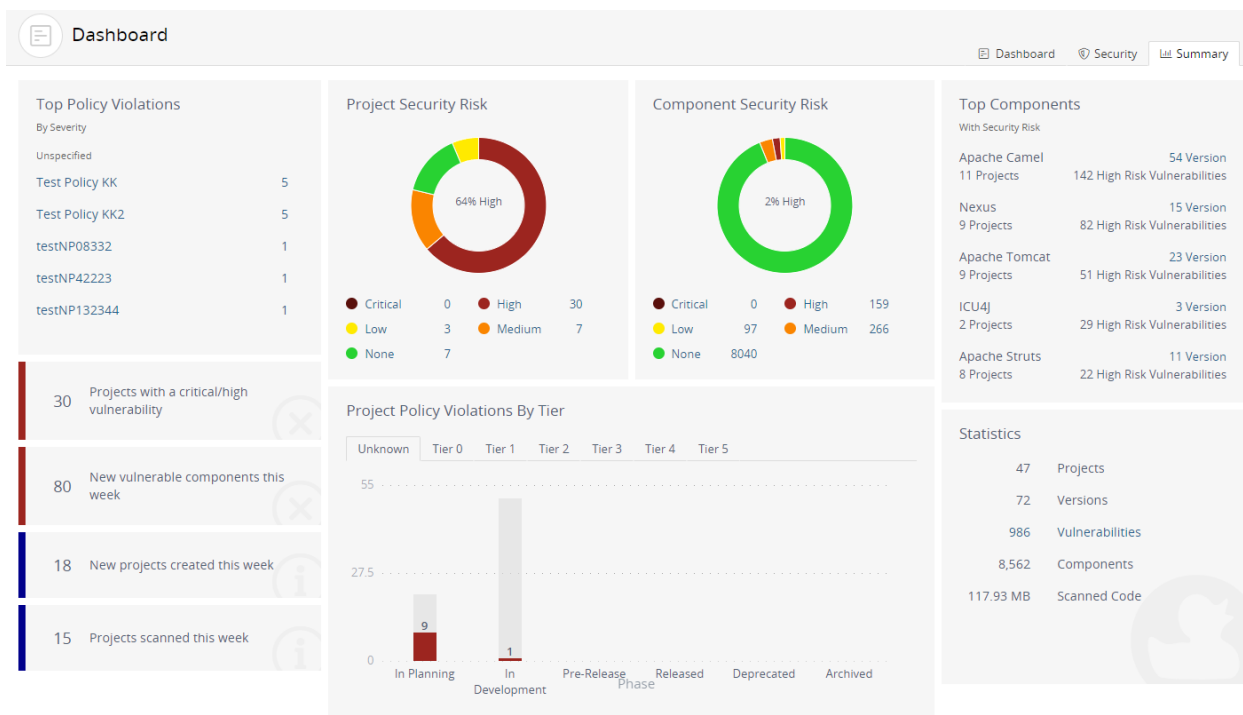
| struts.apache.org Apache Struts ▸ 2.3.7 java Versions: 176 | | Security Cryptography Copyrights Details Settings |
|---|--------------|---|
| Filter Vulnerabilities... | | |
| Identifier | Published | Overall Score ▾ |
| > NVD CVE-2016-3081 | Apr 26, 2016 | 9.3 High |
| > BDSA BDSA-2018-2905 (CVE-2018-11776) | Aug 22, 2018 | 8.3 High |
| > BDSA BDSA-2013-0027 (CVE-2013-4316) | Oct 8, 2018 | 7.4 High |
| > BDSA BDSA-2014-0067 (CVE-2013-2251) | May 24, 2018 | 6.5 Medium |
| > BDSA BDSA-2017-0903 (CVE-2017-9805) | Sep 6, 2017 | 6.2 Medium |
| > BDSA BDSA-2014-0117 (CVE-2014-0094) | Feb 19, 2019 | 6.2 Medium |
| > BDSA BDSA-2013-0028 (CVE-2013-1966) | Oct 9, 2018 | 6.2 Medium |
| > BDSA BDSA-2017-0367 (CVE-2017-9791) | Aug 9, 2017 | 6.2 Medium |
| > BDSA BDSA-2017-0031 (CVE-2017-5638) | Mar 10, 2017 | 6.2 Medium |
| > BDSA BDSA-2017-0954 (CVE-2017-12611) | Sep 11, 2017 | 6.2 Medium |
| > BDSA BDSA-2013-0052 (CVE-2013-2115) | Aug 14, 2019 | 6.2 Medium |
| > BDSA BDSA-2020-2097 (CVE-2019-0230) | Aug 18, 2020 | 5.9 Medium |

- For each component version, the search results also show:
 - Approval status. Status indicates whether this component version has been reviewed.
 - First detected date.

- Date this component version was released.
 - Number of newer versions.
 - Date when a vulnerability for the component was last updated in Black Duck (by updates from the Black Duck KnowledgeBase or a user manually changing the associated vulnerability and so on).
- Manage how the components are shown in these dashboards:
- Use the **Sort by** field to select an attribute to sort by and click an arrow to select the sort order (ascending) or  (descending).
 - Use the filter field to filter the components shown in the dashboard.

Viewing the health of your projects

Use the **Summary** tab to view the overall health of your projects and identify areas of concern. The page consists of widgets that provide business critical information which you can use to quickly assess areas where you need to focus your attention.



Note: The **Summary** tab only displays information for the projects you have permission to view.

The following table describes each widget shown on the **Summary** tab and, where available, how to view additional information. Note that the security risk values shown use CVSS v2 or CVSS v3.x scores, depending on which security risk calculation you selected; by default CVSS v2 scores are shown. Note that the graphs display a Critical risk category with a value of 0, if you selected CVSS 2.0.

| Description | More Information |
|---|---|
| <p>The Top Policy Violations widget displays up to the top five policy violations across all projects that you have permission to view.</p> <p>Policy rules are listed by severity level and then by the number of policy violations, in descending order. If policy rules do not have severity levels assigned to them, the widget displays the top five policy violations, in descending order by the number of violations.</p> <ul style="list-style-type: none"> • If you do not have the Policy Management module, this widget will not appear on the page. • A message appears if you have the Policy Management module but do not have any policy rules configured or have any policy violations. | <p>Select a policy rule to view the My Projects tab filtered to display the projects with a version that violates that policy rule.</p> |
| <p>The Project Security Risk widget displays the number of projects you have permission to view for each level of security risk.</p> <p>Note that this widget counts the highest security risk level for a project, not all security levels affecting a project. For example, if a project has medium and low security risks, it is counted as a project with medium security risk; it is not included as a project with low security risks.</p> | <p>Select a value to view the My Projects tab of the Dashboard page filtered to display the projects that have that security risk level as the highest security risk.</p> <p>Hover over the graph to view the number of projects with that level of security risk.</p> |
| <p>The Component Security Risk widget displays the number of components in projects you have permission to view for each security risk level.</p> <p>Note that the widget counts only the highest security risk for a component. For example, if a component has medium and low security risks, it is counted as one component with a medium security risk.</p> | <p>Select a value to open the Components tab of the Find page filtered to show the components with the selected security risk.</p> <p>Hover over the graph to view the number of components with that level of security risk.</p> |
| <p>The Top Components with Security Risk widget displays up to the top five components used in the projects you have permission to view. The information shown for each component is:</p> <ul style="list-style-type: none"> • Component name and number of versions used in your projects. If only one version is used, the specific version is listed here. • Number of your projects that have this component. • Number of security risks in this component, with the highest security risk listed here. <p>Components are organized by security risk, with those components with the highest risk listed first.</p> | <p>Select the specific version to view the Details tab of the <i>Component Name Version</i> page.</p> <p>Select the number of versions to view the Overview tab of the <i>Component Name</i> page.</p> |
| <p>The Projects have a critical/high vulnerability widget displays the number of projects with versions that contain components with a critical and/or high security risk.</p> | <p>N/A.</p> |

| Description | More Information |
|---|---|
| The New vulnerable components this week widget displays the number of components the Black Duck KB mapped a vulnerability to in the past seven days, including today. | N/A. |
| The New projects created this week widget displays the number of projects that you have permission to view that have been created in the past seven days, including today. | N/A. |
| The Projects scanned this week widget displays the number of projects with scans from the past seven days, including today. | N/A. |
| <p>The Project Policy Violations by Tier widget displays the total number of projects by phase that have a policy violation, grouped by tiers.</p> <ul style="list-style-type: none"> • If you do not use tiers for your projects, projects are grouped in a single category called Unknown. • If you do not have the Policy Management module, this widget displays Projects by Tier. | For each tier, hover over a bar to see the number of projects in this phase and the number of projects in this phase with a policy violation. |
| <p>The Statistics widget displays the following information:</p> <ul style="list-style-type: none"> • Projects lists the number of your projects. • Versions lists the number of project versions for your projects. • Vulnerabilities lists the number of vulnerabilities in your projects. • Components lists the number of components used in your projects, <i>including ignored components</i>. • Scanned Code lists the number of GBs scanned for all scans. | Select the vulnerability value to view the Security tab filtered to show the vulnerabilities with a New, Needs Review, or Remediation Required status. |

About security risk

Black Duck helps security and development teams identify security risks across their applications.

By mapping vulnerabilities to your open source software, Black Duck can provide you with high-level overview information on security risk of your projects, along with detailed information on security vulnerabilities which you can use to investigate and remediate your security vulnerabilities.

Vulnerabilities are linked to the open source components by the Common Vulnerabilities and Exposures numbers (CVEs), as reported in the National Vulnerabilities Database (NVD) maintained by the National Institutes of Standards and Technology (NIST) and/or by (BDSA) numbers If you have licensed Black Duck Security Advisories.

Security risk levels

NVD and BDSA use the Common Vulnerability Scoring System (CVSS) which provides a numerical score reflecting the severity of a vulnerability. The numerical score is then translated into a risk level to help you assess and prioritize security vulnerabilities.

Black Duck provides you with the option of viewing CVSS v2 or CVSS v3.x scores. By default, Black Duck displays CVSS v2 scores.

- CVSS v2 scores has the following values:

- Low risk: 0.0 - 3.9
- Medium risk: 4.0 - 6.9
- High risk: 7.0-10.0

Note that Black Duck shows vulnerabilities with a 0.0 score as no risk.

Although CVSS v2 does not have a Critical risk category, the security graphs In the Black Duck UI display a Critical risk category. This category will display a value of 0 for CVSS v2.

- CVSS v3.x scores has the following values:

- None: 0.0
- Low risk: 0.1 - 3.9
- Medium risk: 4.0 - 6.9
- High risk: 7.0 - 8.9
- Critical risk: 9.0 - 10.0

Note that the scores shown for CVSS v3.x can be v3.0 or v3.1 scores.

Suggested work flow

To manage security risk using Black Duck:

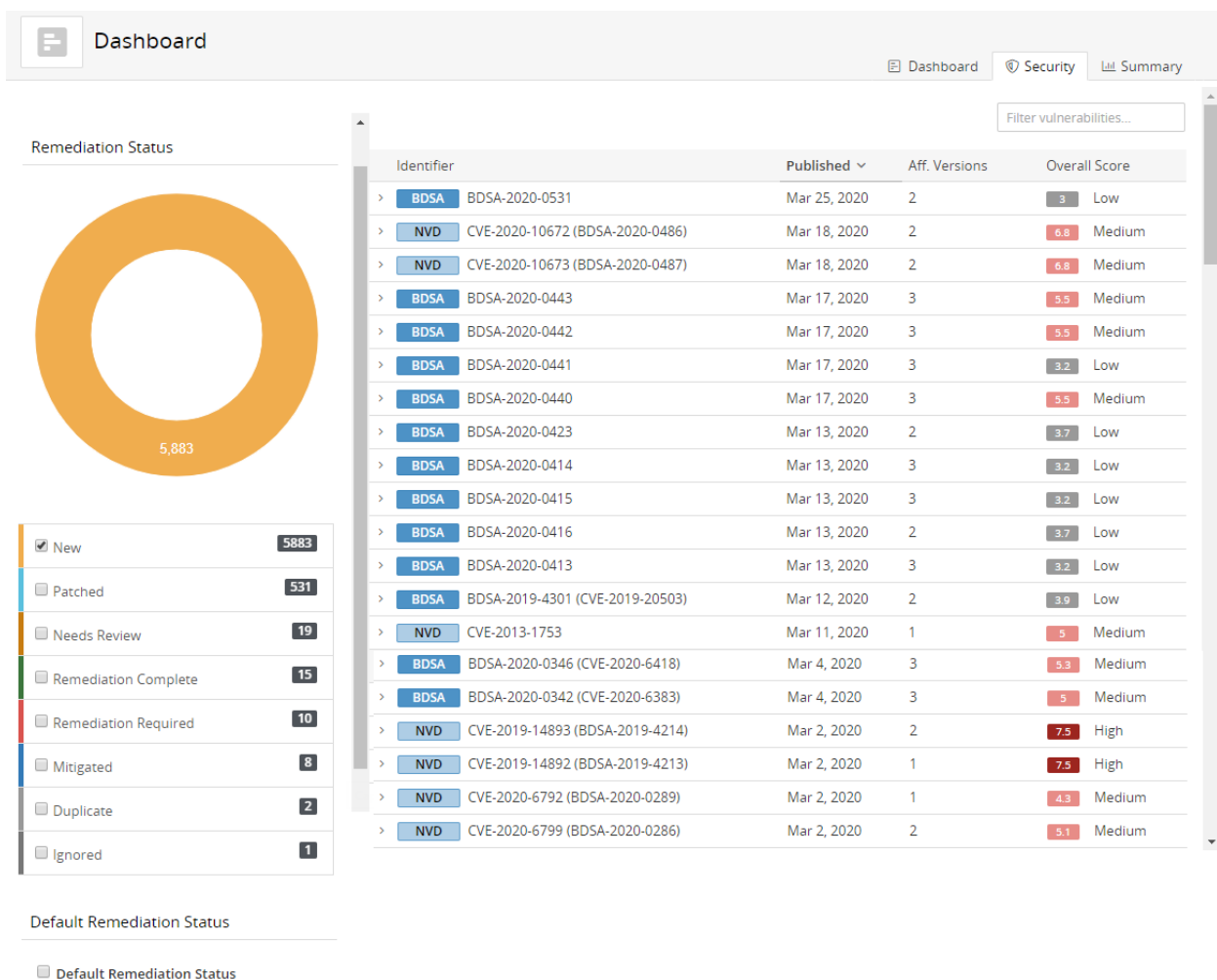
1. With the assistance of your security team, determine your security risk policies.
2. If necessary, users with the system administrator role can define the default security risk calculation.
3. Create policies that trigger violations when components do not comply with your security policies.
4. Depending on your interests:
 - Use the Summary Dashboard to view the overall health of your projects and identify areas of concern. Use this page to quickly assess areas where you need to focus your attention.
 - Use these pages for a high-level overview information of security risk:
 - Dashboard to view the overall security risk across all your projects and components used in your projects.
 - Security Dashboard to view the security risk associated with all the vulnerabilities that exist in your projects. This dashboard also shows the remediation status of all the vulnerabilities that exist within the projects.
 - Use these pages for project version-level information:
 - project version page/**Components** tab, also known as the project version BOM, to view the components specific to that project version, that have security risk.
 - project version page/ **Security** tab to view the security vulnerabilities of each severity associated with the components used in a project version.
5. Investigate vulnerabilities and policy violations. For detailed information on security vulnerabilities, view the:
 - CVE page

- BDSA page if you have licensed Black Duck Security Advisories (BDSA)
6. After reviewing the severity of the vulnerability, users with the appropriate role can change the remediation status of the security vulnerability.
 7. Monitor notifications for any new security vulnerabilities.

You will receive notification alerts if security vulnerabilities are published or updated against components that are included in one or more of your projects.

Viewing all security vulnerabilities

Use the Security Dashboard to identify and manage risk. This dashboard lists all the security vulnerabilities that affect your projects.



Using the Security Dashboard is an efficient way to:

- Identify the remediation status of all the vulnerabilities in your projects.
- Review the severity of the vulnerability to determine if remediation is required.

Note: The security risk values shown use CVSS v2 or CVSS v3.x scores, depending on which security risk calculation you selected; by default CVSS v2 scores are shown.

⚙️ To use the Security Dashboard to identify and manage risk

1. Log in to Black Duck.
2. From the Dashboard, click the **Security** tab to display the Security Dashboard.
3. You can use:
 - The table filter field to filter the vulnerabilities shown in the table by identifier.
 - The **Aff. Versions** column to view the number of project versions affected by this vulnerability. Use this column to identify the vulnerabilities that are affecting the greatest number of versions of your projects.
 - The Remediation Status chart to view the remediation status of all vulnerabilities that exist within all projects and the number of vulnerabilities with each remediation status.

By default, the chart displays all remediation statuses. Clear the check box to hide the vulnerabilities with that remediation status.
 - The **Overall Score** column shows the Temporal score (for BDSA), or Base score (for NVD) and associated risk level. Hover over the **Overall Score** value to see the individual values.
 - For BDSA, the Temporal, Base, Exploitability, and Impact scores are shown.
 - For NVD, the Base, Exploitability, and Impact scores are shown.
 - The table to view more information on a vulnerability by selecting > next to the vulnerability that interests you.

| | |
|--|---|
| Description IBM Jazz Foundation (IBM Rational Engineering Lifecycle Manager 5.0 through 6.0.6) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 152740. View CVE record | Base Score Metrics <div> AV: NETWORK AC: MEDIUM AU: SINGLE </div> <div> A: NONE C: NONE I: PARTIAL </div> <div> Published on Mar 14, 2019 Last Modified Apr 15, 2019 </div> |
|--|---|

Select to view the BDSA record and/or the CVE record from which you can remediate the vulnerability, if you have the appropriate role.

Note: A single vulnerability can be present multiple times in the remediation status pie chart since it can have multiple different remediation types within a single BOM or across multiple project version BOMs. However, a single vulnerability is listed in only one row in the table.

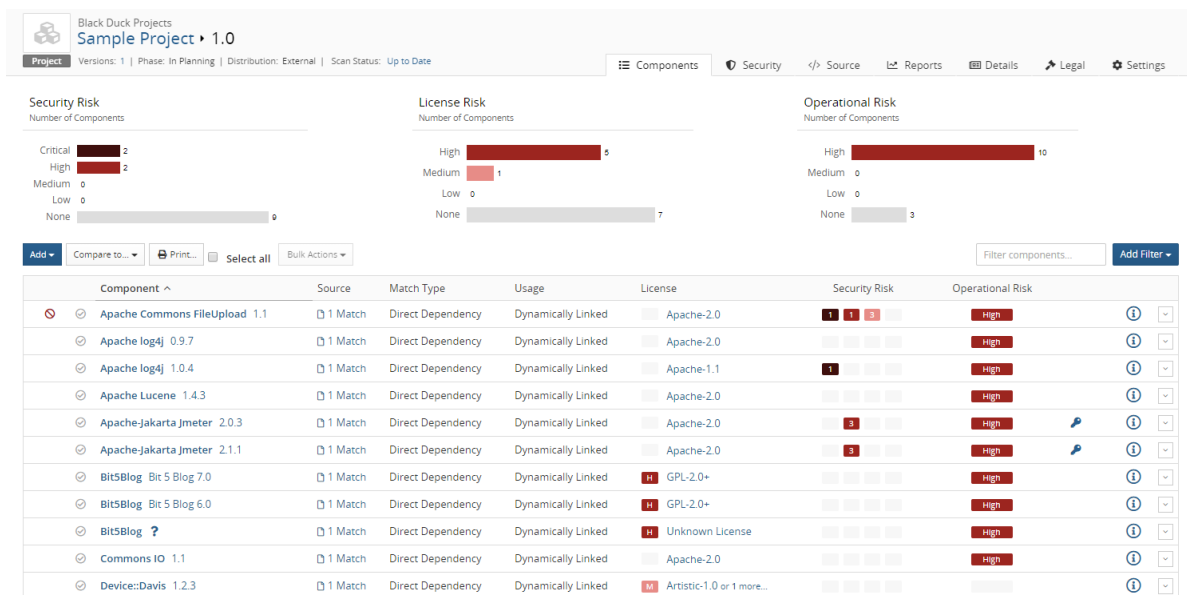
Chapter 4: Viewing your BOM

Once you have mapped a component scan to a project version, the results automatically create the project version's BOM.

⚙️ To view a project version's BOM

1. Log in to Black Duck.
2. Select the project name using the **Watching** or **My Projects** dashboard. The *Project Name* page appears.
3. Select the version name of the project that you want to view.

The **Components** tab shows you the BOM.



By default, the BOM displays a "flat" view of components where all components found are listed at the same level. Select **Component Tree** to view a hierarchical view which is based on file system relationships.

Adjusting the component and/or component version in a BOM

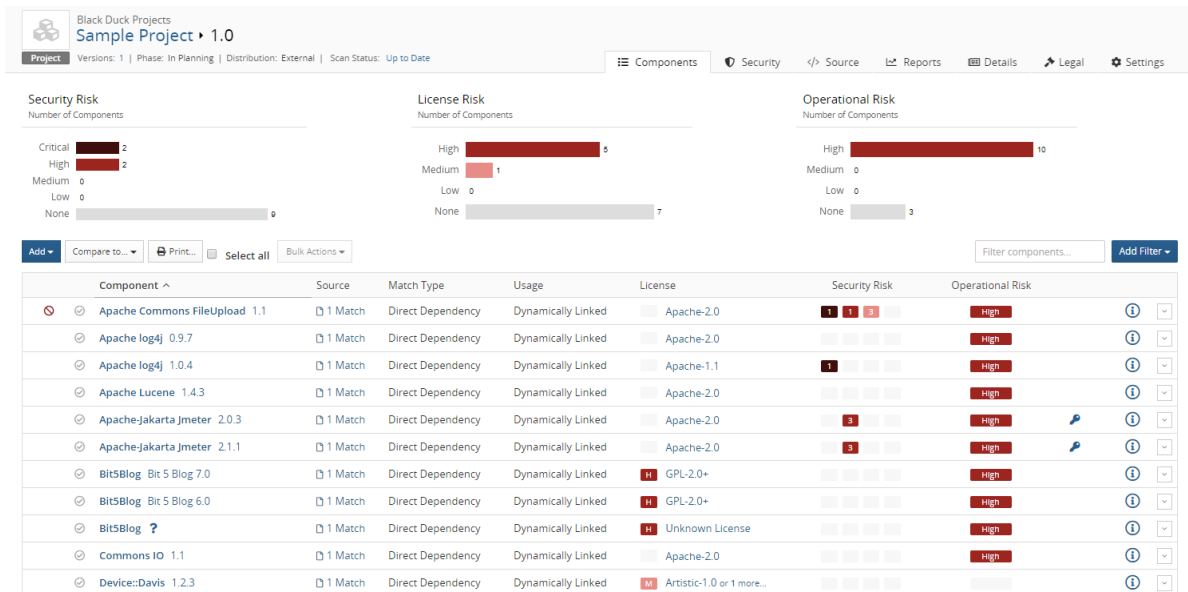
Once you have mapped a component scan to a project version, the scan results automatically create the project version's BOM. Although component scanning automatically discovers the open source component and

component version from most archive files by comparing them to components in the Black Duck KB, you may be using a version of the component that is not available in the Black Duck KB, or you may be using a modified version of a component. You can adjust the component and version for a component in a BOM.


- If the component/version is available in the Black Duck KB, users with the appropriate role can adjust the component or component version, as described below.
- If the component version of a component is not available in the Black Duck KB, users with the Component Manager role can create a custom version and add it to the BOM.


To select an alternate component and/or version match for a component in a BOM

1. Log in to Black Duck.
2. Select the project name using the **Watching** or **My Projects** dashboard. The *Project Name* page appears.
3. Select the version name to open the **Components** tab and view the BOM.



| Component | Source | Match Type | Usage | License | Security Risk | Operational Risk |
|-------------------------------|---------|-------------------|--------------------|---------------------------|---------------|------------------|
| Apache Commons FileUpload 1.1 | 1 Match | Direct Dependency | Dynamically Linked | Apache-2.0 | High | High |
| Apache log4j 0.9.7 | 1 Match | Direct Dependency | Dynamically Linked | Apache-2.0 | High | High |
| Apache log4j 1.0.4 | 1 Match | Direct Dependency | Dynamically Linked | Apache-1.1 | High | High |
| Apache Lucene 1.4.3 | 1 Match | Direct Dependency | Dynamically Linked | Apache-2.0 | High | High |
| Apache-Jakarta Jmeter 2.0.3 | 1 Match | Direct Dependency | Dynamically Linked | Apache-2.0 | High | High |
| Apache-Jakarta Jmeter 2.1.1 | 1 Match | Direct Dependency | Dynamically Linked | Apache-2.0 | High | High |
| BitSBlog Bit 5 Blog 7.0 | 1 Match | Direct Dependency | Dynamically Linked | GPL-2.0+ | High | High |
| BitSBlog Bit 5 Blog 6.0 | 1 Match | Direct Dependency | Dynamically Linked | GPL-2.0+ | High | High |
| BitSBlog ? | 1 Match | Direct Dependency | Dynamically Linked | Unknown License | High | High |
| Commons IO 1.1 | 1 Match | Direct Dependency | Dynamically Linked | Apache-2.0 | High | High |
| Device:Davis 1.2.3 | 1 Match | Direct Dependency | Dynamically Linked | Artistic-1.0 or 1 more... | High | High |

4. In the component list view of the BOM, click  and select **Edit** to open the Edit component dialog box.
5. Type the name of the OSS component in the **Component** field and select the alternate match.
6. Select the version of the component from the **Version** list. The list contains all versions of the component that are available in the Black Duck KB.
7. Optionally, enter a purpose for this adjustment and/or select the **Modification** checkbox and optionally, enter information regarding this modification in the field.
8. Click **Save**.

The component and version for the BOM entry are updated. The Information indicator () appears in the table row to indicate that the component and/or version were changed from the one automatically

discovered in the component scan:

| <div> <div></div> <div></div> </div> | | <div>Add</div> | <div>Bulk Actions</div> | <div>Compare to...</div> | <div>Print...</div> | <div>Match Status</div> <div>Confirmed</div> <div>×</div> | <div>Ignore</div> <div>Not ignored</div> <div>×</div> | <div>Filter components...</div> | <div>Add Filter</div> |
|---|--|--------------------|----------------------------|-------------------------------|--------------------------|---|---|---------------------------------|-----------------------|
| Component ^ | | Source | Match Type | Usage | License | Security Risk | | Operational Risk | |
| <div> <div></div> <div>AOP Alliance (Java/JZEE AOP standard) 1.0</div> </div> | | <div>1 Match</div> | <div>Exact Directory</div> | <div>Dynamically Linked</div> | <div>Public Domain</div> | <div></div> <div></div> <div></div> | | <div>High</div> | |

Selecting a different license for a component in a BOM

You can select a license for a component used in a BOM that is different from the component's declared license that is identified in the Black Duck KB.

⚙ To select a different license for an OSS component in the project version's BOM

1. Log in to Black Duck.
2. Select the project name using the **Watching** or **My Projects** dashboard. The *Project Name* page appears.
3. Select the version name to open the **Components** tab and view the BOM.
4. Select the existing license to open the *Component Name Version* Component License dialog box.

Component Name Version

Component License

Attribution Statement >

License

Apache License 2.0

Apache License 2.0 (Apache-2.0)

Apache License 2.0

Status: Unreviewed | Family: Permissive

Permitted

> Private Use

> Place Warranty

> Modify

> Distribute

> Commercial Use

Forbidden

> Test Term

> Hold Liable

> Use Trademarks

Required

> State Changes

> Include Notice

Apache License

Version 2.0, January 2004

=====

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.


"Legal Entity" shall mean the union of the acting entity and all other entities

Close

Save Changes

5. Backspace to clear the field and then type the name of the license that you want to assign, and from the list of suggestions, select the one you want.
6. Click **Save Changes**.

The assigned license is updated. If the new license carries a different type of license risk than the previous one, the license risk calculations for the component and for the project version are updated. A

 appears in the table row to indicate that a manual adjustment was made to this component.

SYNOPSYS

Page | 49

Black Duck 2020.10.0