



Getting Started

Black Duck 2024.7.3

Copyright ©2024 by Black Duck.

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.

12-11-2024

Contents

Preface	4
Black Duck documentation.....	4
Customer support.....	4
Black Duck Community.....	5
Training.....	5
Black Duck Statement on Inclusivity and Diversity.....	5
Black Duck Security Commitments.....	6
1. About Black Duck	7
2. Logging in to Black Duck	8
3. Scanning your code	9
Using Black Duck Detect (Desktop).....	9
Creating a project.....	23
Mapping a scan to a project.....	25
4. Viewing risk in Black Duck	28
Dashboards.....	28
Project version pages.....	30
Viewing your dashboards.....	31
Viewing the health of your projects.....	42
About security risk.....	48
Security risk levels.....	48
Estimated Security Risk.....	49
Suggested work flow.....	49
5. Viewing your BOM	51
Adjusting the component and/or component version in a BOM.....	51

Preface

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.

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

- [Helm](#) is a package manager for Kubernetes that you can use to install Black Duck. Black Duck supports Helm3 and the minimum version of Kubernetes is 1.13.

Black Duck integration documentation is available on:

- <https://sig-product-docs.blackduck.com/bundle/integrations-detect/page/integrations/integrations.html>
- https://documentation.blackduck.com/category/cicd_integrations

Customer support

If you have any problems with the software or the documentation, please contact Black Duck Customer Support:

- Online: <https://community.blackduck.com/s/contactsupport>
- To open a support case, please log in to the Black Duck Community site at <https://community.blackduck.com/s/contactsupport>.
- Another convenient resource available at all times is the [online Community portal](#).

Black Duck Community

The Black Duck 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 Black Duck 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 Black Duck product users to allow you to learn valuable lessons from a diverse group of industry leading companies. In addition, the Customer Hub puts all the latest product news and updates from Black Duck at your fingertips, helping you to better utilize our products and services to maximize the value of open source within your organization.
- **Solve** – Quickly and easily get the answers you're seeking with the access to rich content and product knowledge from Black Duck experts and our Knowledgebase.
- **Share** – Collaborate and connect with Black Duck staff and other customers to crowdsource solutions and share your thoughts on product direction.

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

Training


Black Duck Customer Education 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.

In Black Duck Education, 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://blackduck.skilljar.com/page/black-duck> or for help with Black Duck, select **Black Duck**

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

Black Duck Statement on Inclusivity and Diversity

Black Duck is committed to creating an inclusive environment where every employee, customer, and partner feels welcomed. We are reviewing and removing exclusionary language from our products and supporting customer-facing collateral. Our effort also includes internal initiatives to remove biased language from our

engineering and working environment, including terms that are embedded in our software and IPs. At the same time, we are working to ensure that our web content and software applications are usable to people of varying abilities. You may still find examples of non-inclusive language in our software or documentation as our IPs implement industry-standard specifications that are currently under review to remove exclusionary language.

Black Duck Security Commitments

As an organization dedicated to protecting and securing our customers' applications, Black Duck is equally committed to our customers' data security and privacy. This statement is meant to provide Black Duck customers and prospects with the latest information about our systems, compliance certifications, processes, and other security-related activities.

This statement is available at: [Security Commitments | Black Duck](#)

1. About Black Duck

Black Duck offers a comprehensive suite of services and tools that support customers on their security journey. From customers just starting with security, to customers strengthening an established program, Black Duck has the expertise, skills, and products necessary for success.




Black Duck, a Software Composition Analysis (SCA) tool, helps with managing the supply chain of software, understanding the third-party components in use and minimizing risks from known vulnerabilities and licensing. Black Duck is a comprehensive solution for supply chain management, based primarily on source analysis.

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.


2. Logging in to Black Duck

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.

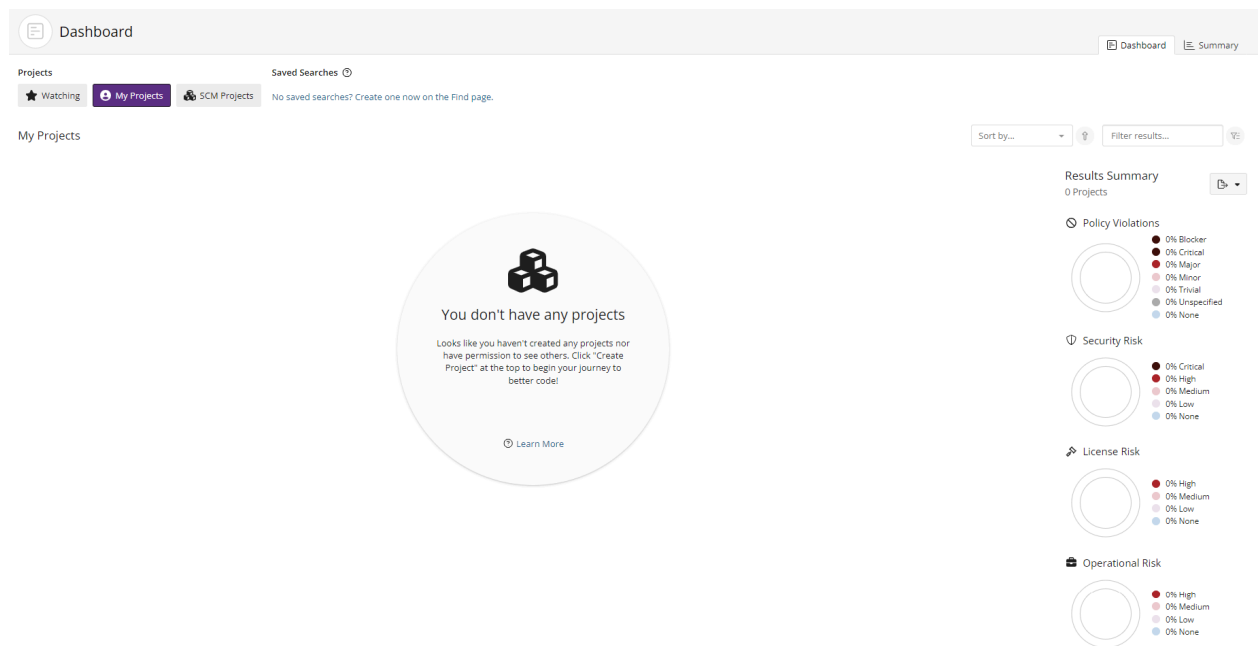
To log in to Black Duck:

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. Your password is case sensitive.

 **Note:** If your administrator has enabled password requirements and your password does not meet the requirements, a dialog box appears notifying you that you must change your password. When updating your password, make sure that it meets the requirements, as listed in the dialog box. You will not be able to log in to Black Duck unless the password meets *all* requirements.

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.



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.

3. Scanning your code

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.

Black Duck provides these scanning tools:

- Black Duck Detect. [Black Duck Detect](#) is the recommended scanning tool for Black Duck.
- 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 Black Duck Detect, Rapid Scanning quickly returns results as it only employs package manager scanning and does not interact with the Black Duck server database. Refer to the Black Duck online help or User Guide for more information about Rapid Scanning.
- Black Duck Detect (Desktop), as described below.
- Command line (CLI) version of Signature Scanner. Refer to the Black Duck online help or User Guide for more information.

Using Black Duck Detect (Desktop)


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

With Black Duck 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 Black Duck Detect (Desktop):

1. Download and install Black Duck Detect (Desktop).
2. Configure Black Duck Detect (Desktop) with your Black Duck server settings and complete the installation process.
3. Use Black Duck 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.

Be sure that your system meets the system requirements of Black Duck Detect.


- Click [here](#) for the system requirements for the latest version of Black Duck Detect.
- Click [here](#) for the documentation for previous versions of Black Duck Detect. Use this page to find the Black Duck Detect version and view the system requirements.

3. Scanning your code • Using Black Duck Detect (Desktop)

Downloading and installing Black Duck 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 Black Duck Detect (Desktop)** section to download the executable from Google Cloud Storage.
4. Run the executable to install Black Duck Detect (Desktop).

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

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

If the Black Duck 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/Black Duck 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 Black Duck Detect (Desktop) with the Sandbox disabled, enter the following at the command line:

```
blackduck-detect --no-sandbox
```

Command line options for Windows

- Unattended (silent) install for Black Duck Detect

```
./blackduck-detect-latest.exe /S
```
- Installing to a specific directory

```
./blackduck-detect-latest.exe /D=C:\directory
```

Installing the Linux version of Black Duck Detect (Desktop)

1. Download the executable from your Black Duck server, as described in the previous section.
2. Install Black Duck Detect (Desktop):

```
cd Downloads
```

To install on CentOS/RedHat:

```
sudo yum localinstall blackduck-detect-latest.rpm
```

To install on Ubuntu/Debian:

```
sudo apt install ./blackduck-detect-latest.deb
```

3. Change the permission of chrome-sandbox:

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

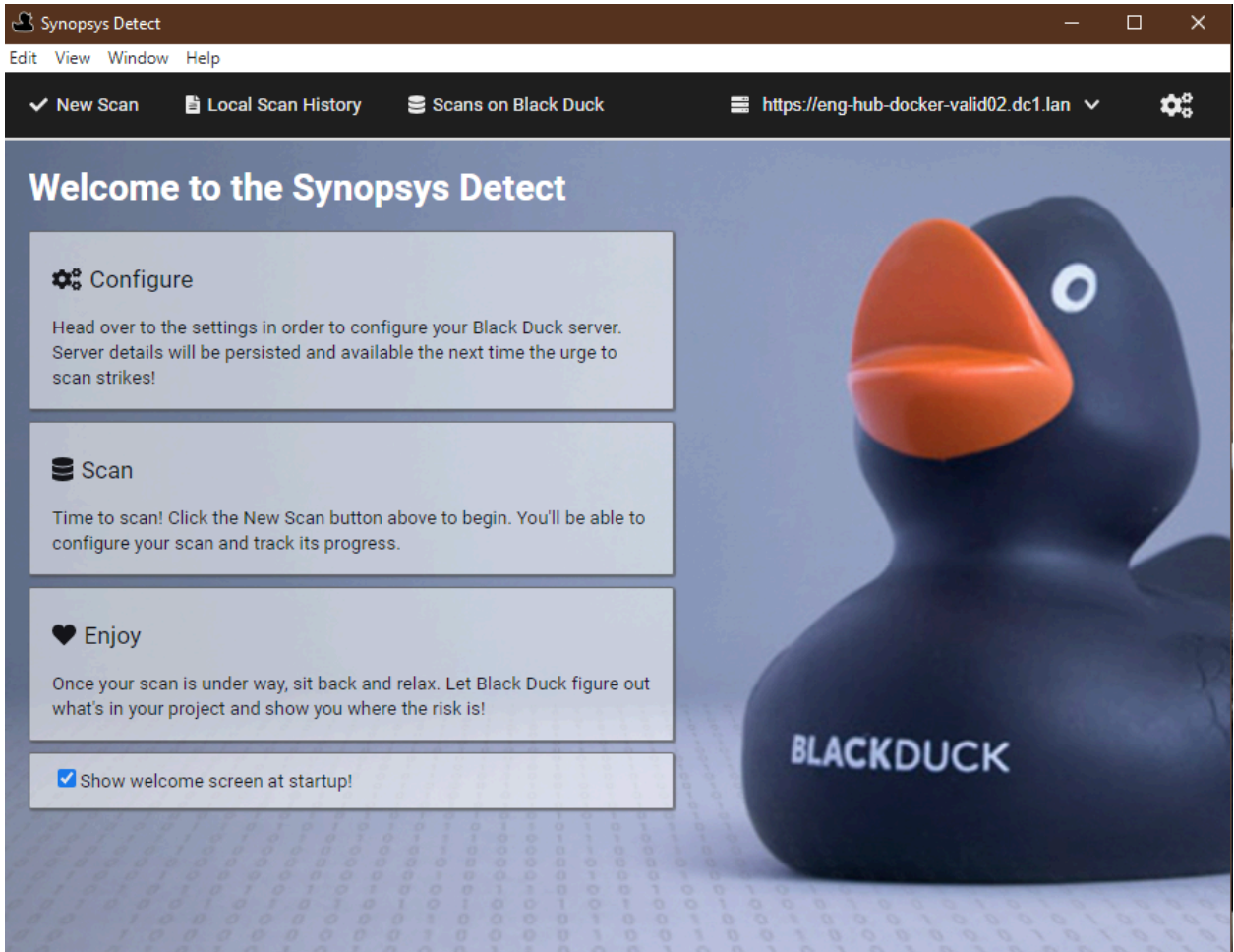
4. Run Black Duck Detect (Desktop):

```
./blackduck-detect --no-sandbox
```

Configuring Black Duck Detect (Desktop)

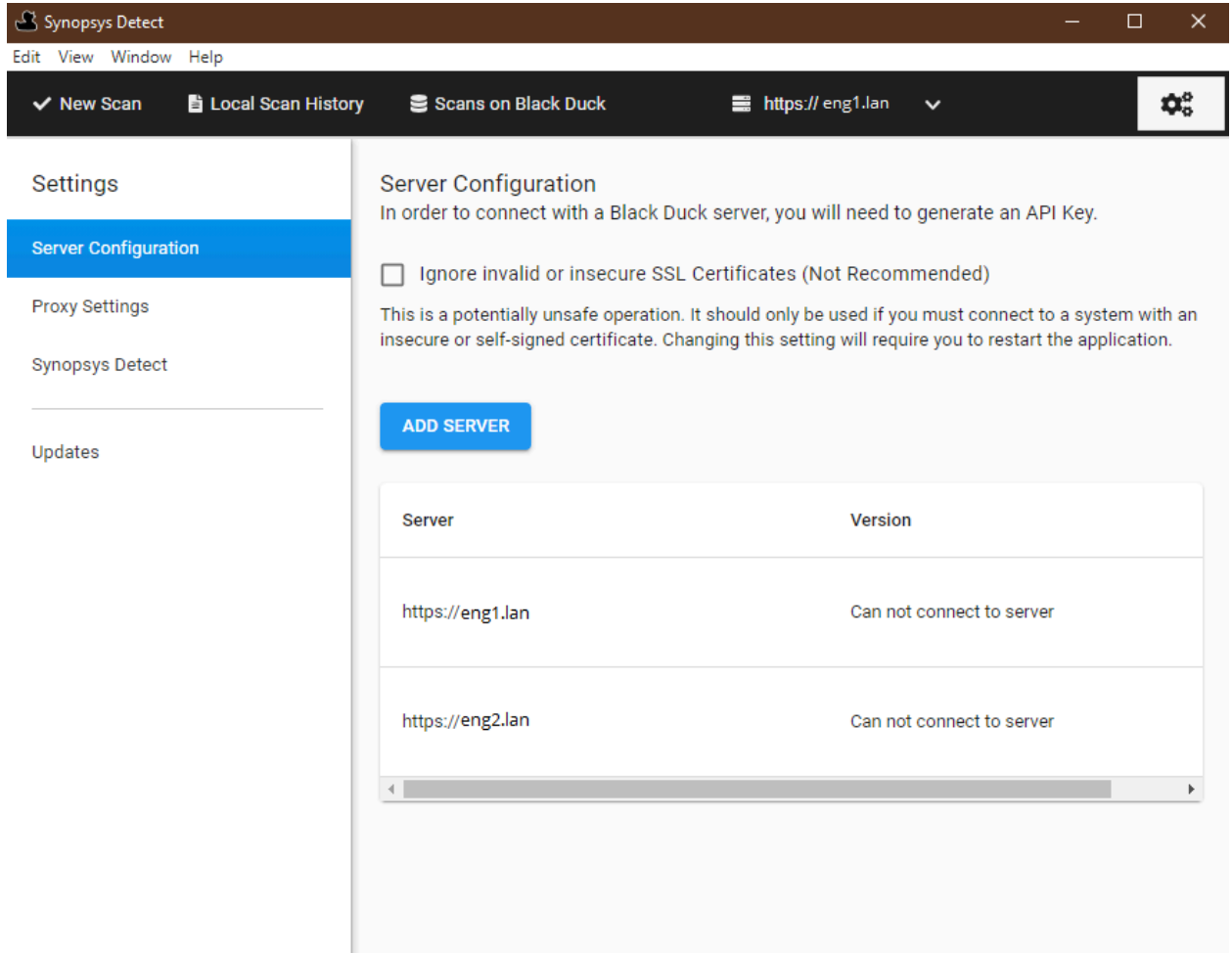
After installing Black Duck Detect (Desktop), continue the installation process by configuring your Black Duck settings.

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



2. Click , located in the upper right corner display the Settings page.

3. Scanning your code • Using Black Duck Detect (Desktop)



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

Black Duck server configuration

To add a server:

1. Select the **Server Configuration** tab and click **Add Server**.
The Add Server dialog box appears.

Add Server

Black Duck Server URL

Generate New API Key

Already have a key?

To generate a new API key, enter your username and password for your Black Duck server. The API key name is used to identify the key and must be unique.

API Key Name

Username *

Password *

CANCEL

CREATE


2. 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.
3. Generate or enter an API key (user access token).
 - To generate a new API key:
 - a. Enter a key name, your username, and password.
 - b. Click **Create**.
 - To enter an API key:
 - a. Select **Already have a key?**
 - b. Enter the API key in the field.
 - c. Click **Create**.
4. Click **Save**. Black Duck Detect (Desktop) connects to the Black Duck server and displays the version of Black Duck you are connected to.

To remove an API key:

Removing the API key does not delete the key in Black Duck. It only removes it locally.

1. Select the **Server Configuration** tab.


3. Scanning your code • Using Black Duck Detect (Desktop)

2. Click  in the row of the server and select **Remove API Key**.

The Remove API Key dialog box appears.

3. Click **OK** to confirm.

To delete a configuration

1. Click  in the row of the server and select **Delete Configuration**.

The Delete Server Configuration dialog box appears.

2. Click **OK** to confirm.

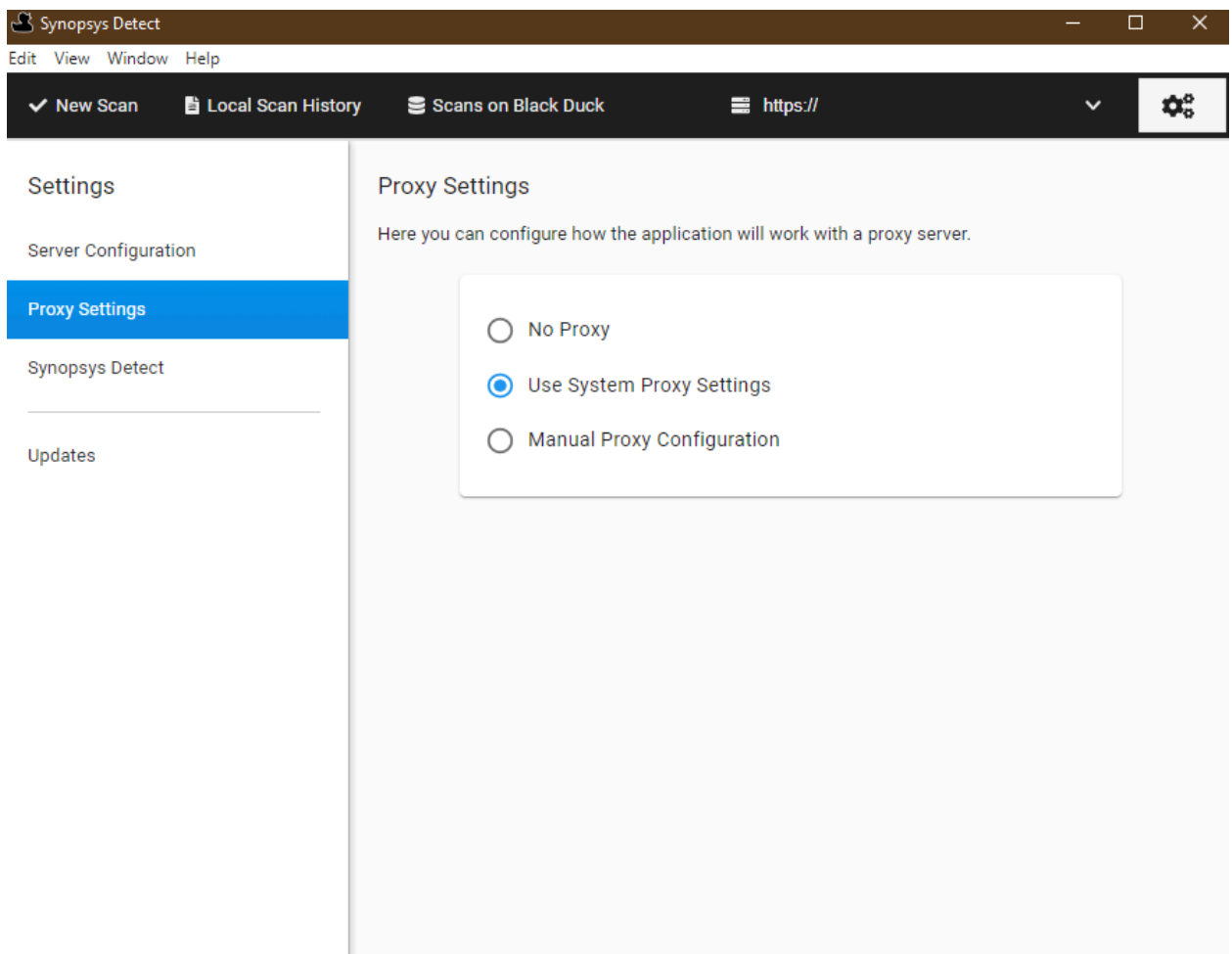
Proxy settings

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

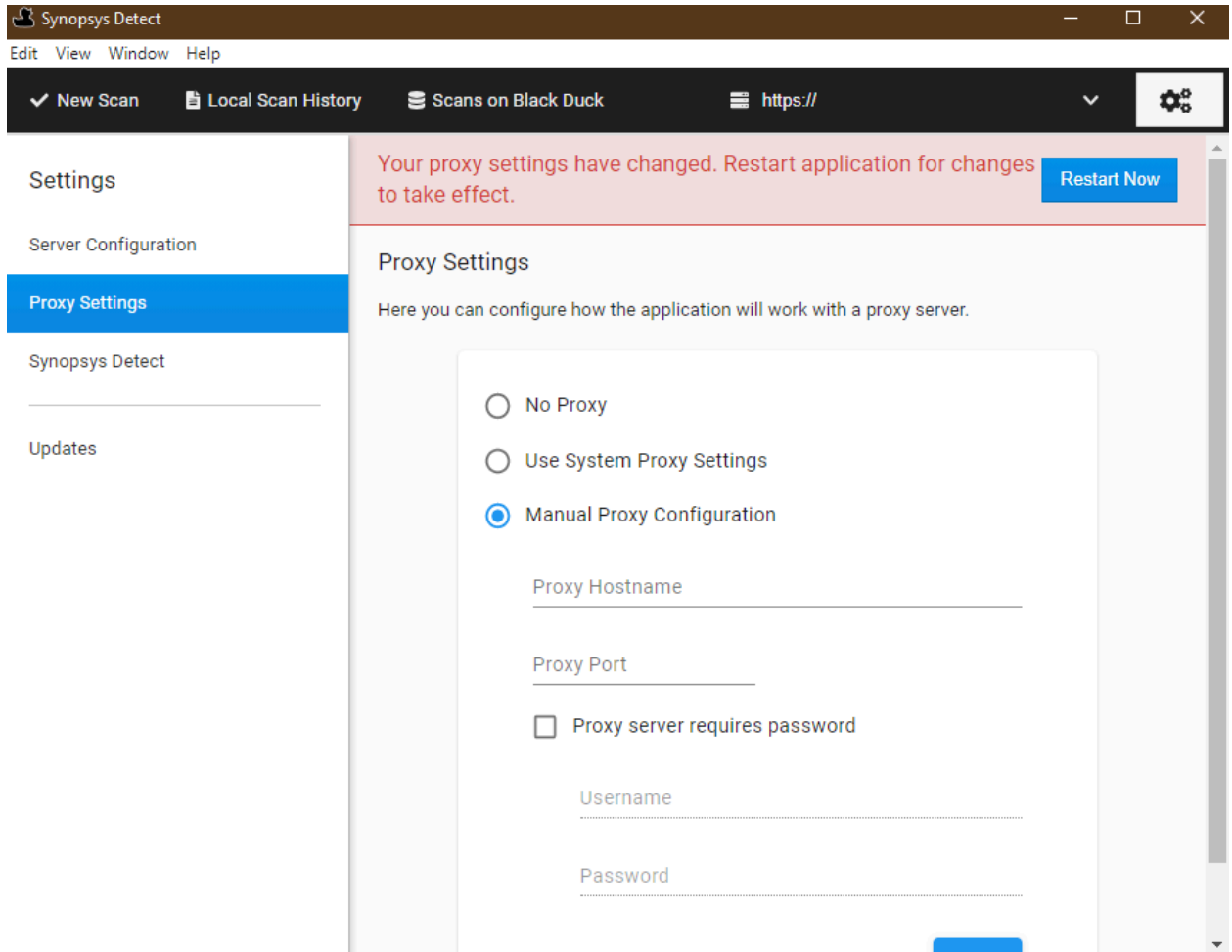
If you are required to manually enter your proxy settings or you do not require a proxy, you can modify these default settings.

To modify the default proxy settings:

1. 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 Black Duck Detect settings


Optionally, select **Synopsys Detect** and if necessary, define any Black Duck 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 Black Duck 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, you can ignore invalid or insecure SSL certificates.

1. Click , located in the upper right corner display the Settings page.
2. Select the **Server Configuration** tab.
3. Check the **Ignore invalid or insecure SSL Certificates** checkbox.
4. Restart the application.

 **CAUTION:** This is a potentially unsafe operation. It should only be used if you must connect to a system with an insecure or self-signed certificate.

Alternatively, if you want to imported a self-signed certificate, this can be done following the standard keytool import process for your JRE.

Identify the location of the JRE being used by Black Duck Detect:


1. Click , located in the upper right corner display the Settings page.
2. Select the **Black Duck Detect** tab.
3. Select **paths** from the Properties menu. Alternatively, type **paths** in the Search Properties search field to narrow the options displayed.
4. If the **Java Executable** field has no value, Black Duck Detect will use the JRE installed under `$JAVA_HOME` set in your system environment variables.

Now that the location of the JRE that Black Duck Detect is using is known, the certificate should be imported to the relevant `cacerts` file (typically found in the `lib\security` folder).

1. Within a terminal session, run the following command (changing the paths to suit):

```
keytool -import -trustcacerts -keystore <path_to_keystore> -file <path_to_certificate> -alias <alias_for_cert>
```

2. You will be prompted for a password. Provide it and press enter.
3. You will be prompted whether or not to trust the certificate. Inspect the contents and accept as appropriate.

 **Note:** It may be necessary to also import any intermediary certificates associated with a chain. If you encounter any issues with the import process, please contact your IT department.

Scanning options

The Black Duck 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 Matching** from the **Scan Settings** options and enable it.
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 **Local 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:


1. Click **New Scan**.
2. From the **What type of scan?** list, select **Binary/Executable**,
3. Click  to select the binary or executable you would like to scan.
4. 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 **Local 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):

1. Click **New Scan**.
2. From the **What type of scan?** list, select **Docker**,
3. Do one of the following:


3. Scanning your code • Using Black Duck Detect (Desktop)

- Enter the Docker image name.
 - Select **Choose Docker archive (.tar)** and click  to select the directory you would like to scan.
4. 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 **Local 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 Black Duck Detect (Desktop) to output the scan to a file which you can later upload to Black Duck by using Black Duck 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**.

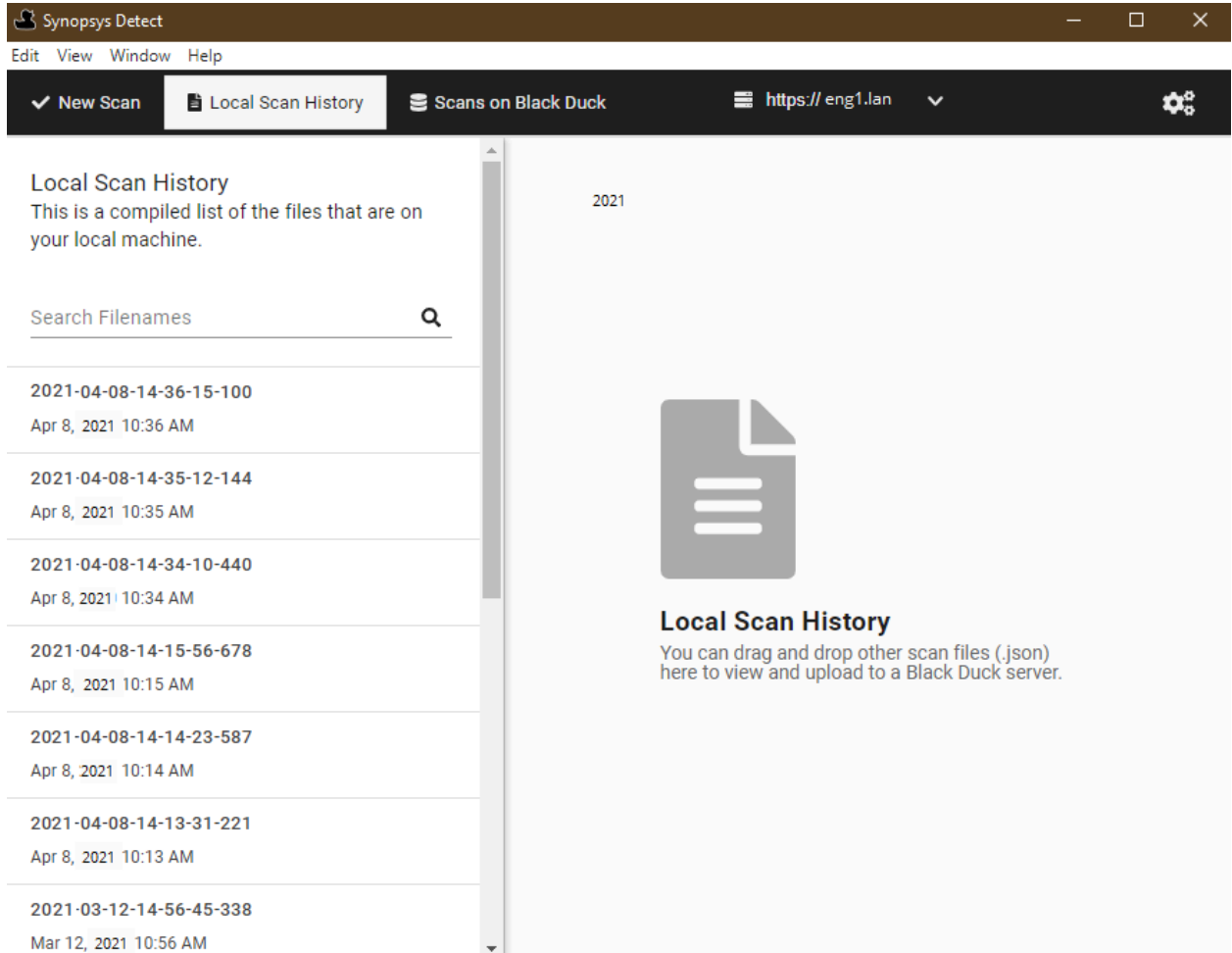
The status of the scan appears along with an option to cancel the scan.
6. When the scan is complete, select the **Local Scan History** tab to view information on the completed scan.

Managing scans

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

1. Click **Local Scan History**.

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

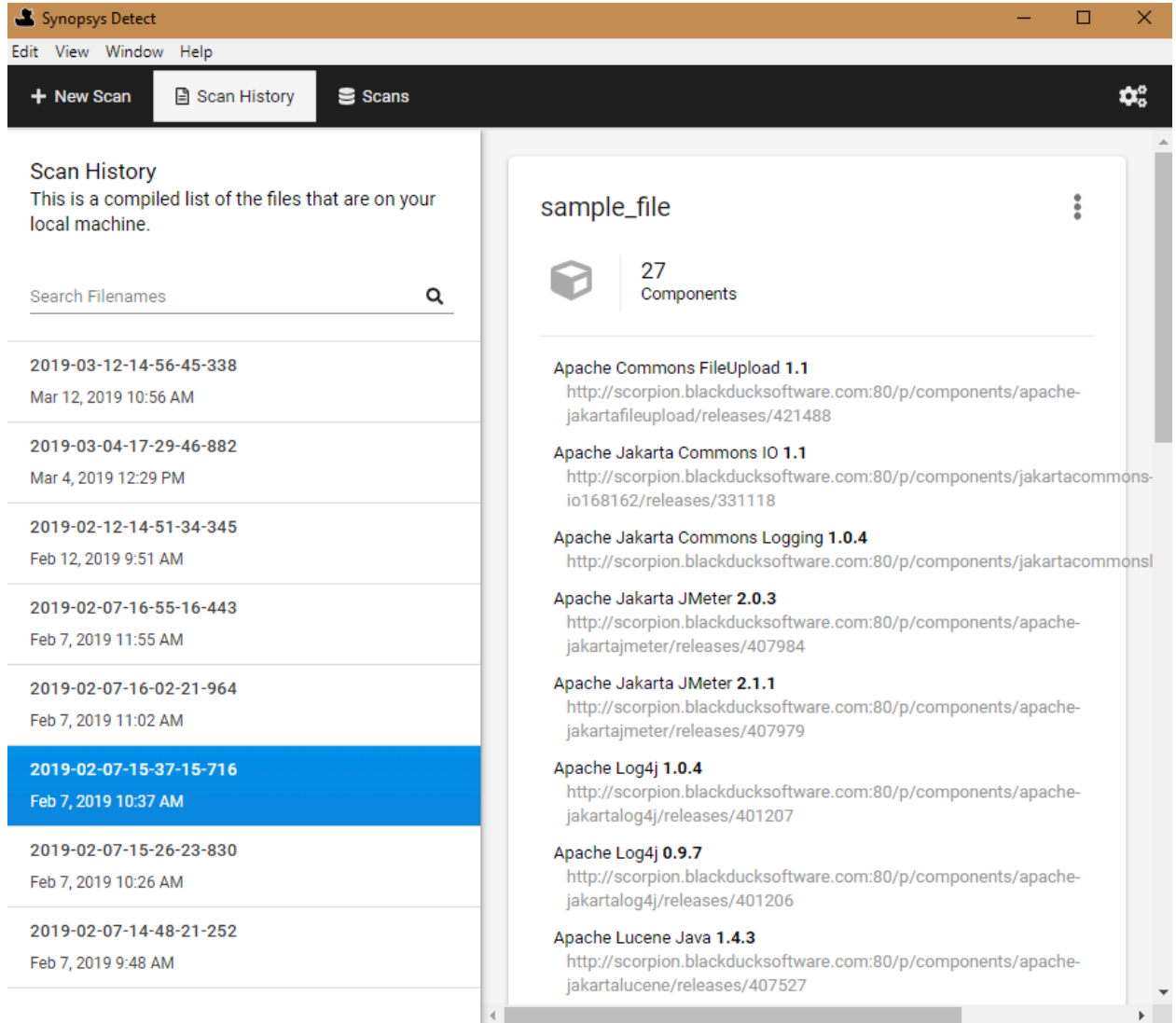



Drag and drop scans from your local machine to this tab to manage them.

From this tab, select a scan and:

- View information on the contents of the scan:

3. Scanning your code • Using Black Duck Detect (Desktop)

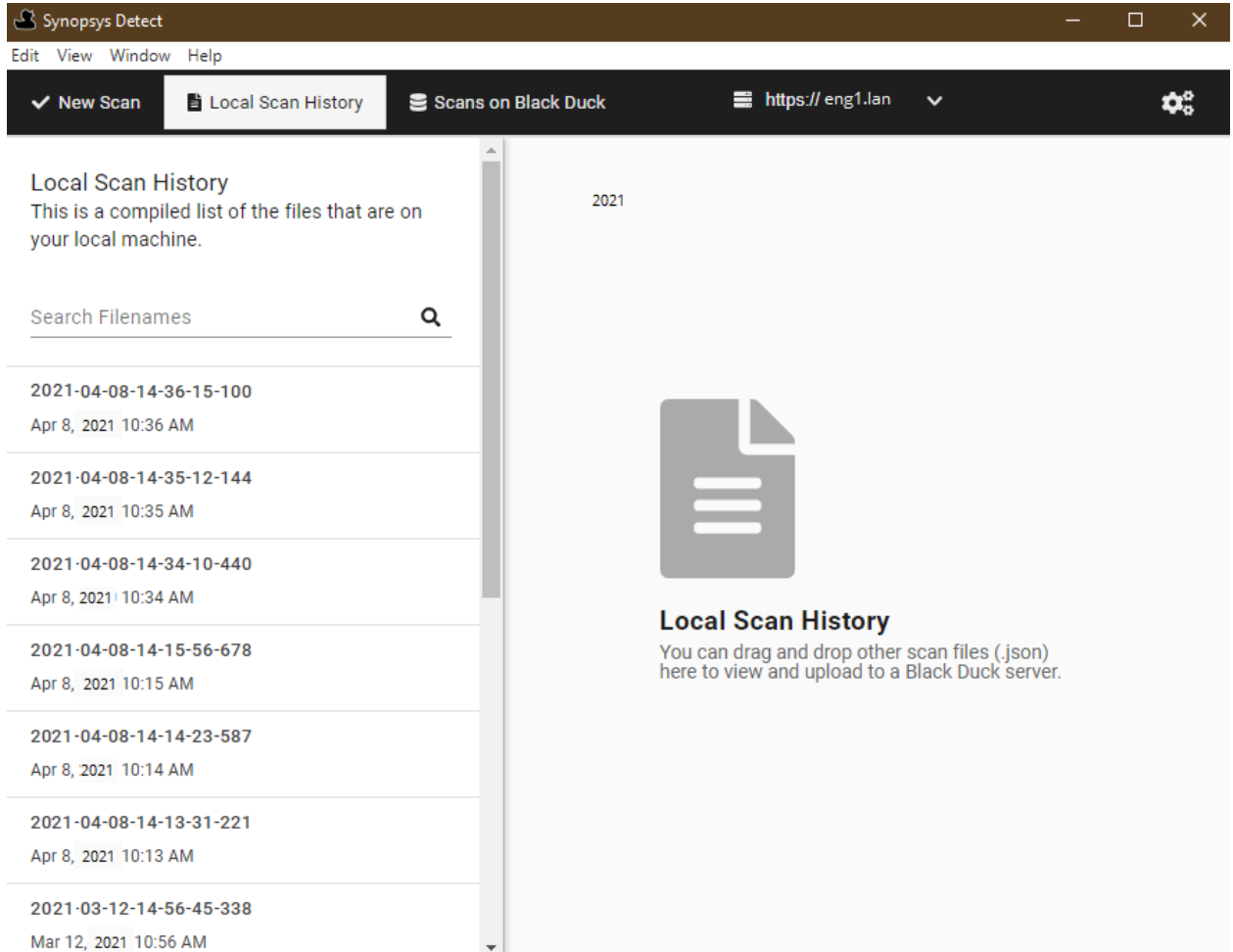



- View the location of the file on your system by clicking  and selecting **Show File**.
- Upload the file, as described in the next section.
- Delete the scan by hovering over the scan name in the left column and clicking **Delete**. Click **Yes** to confirm.

Uploading scan files to Black Duck

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

1. Click **Local Scan History**.



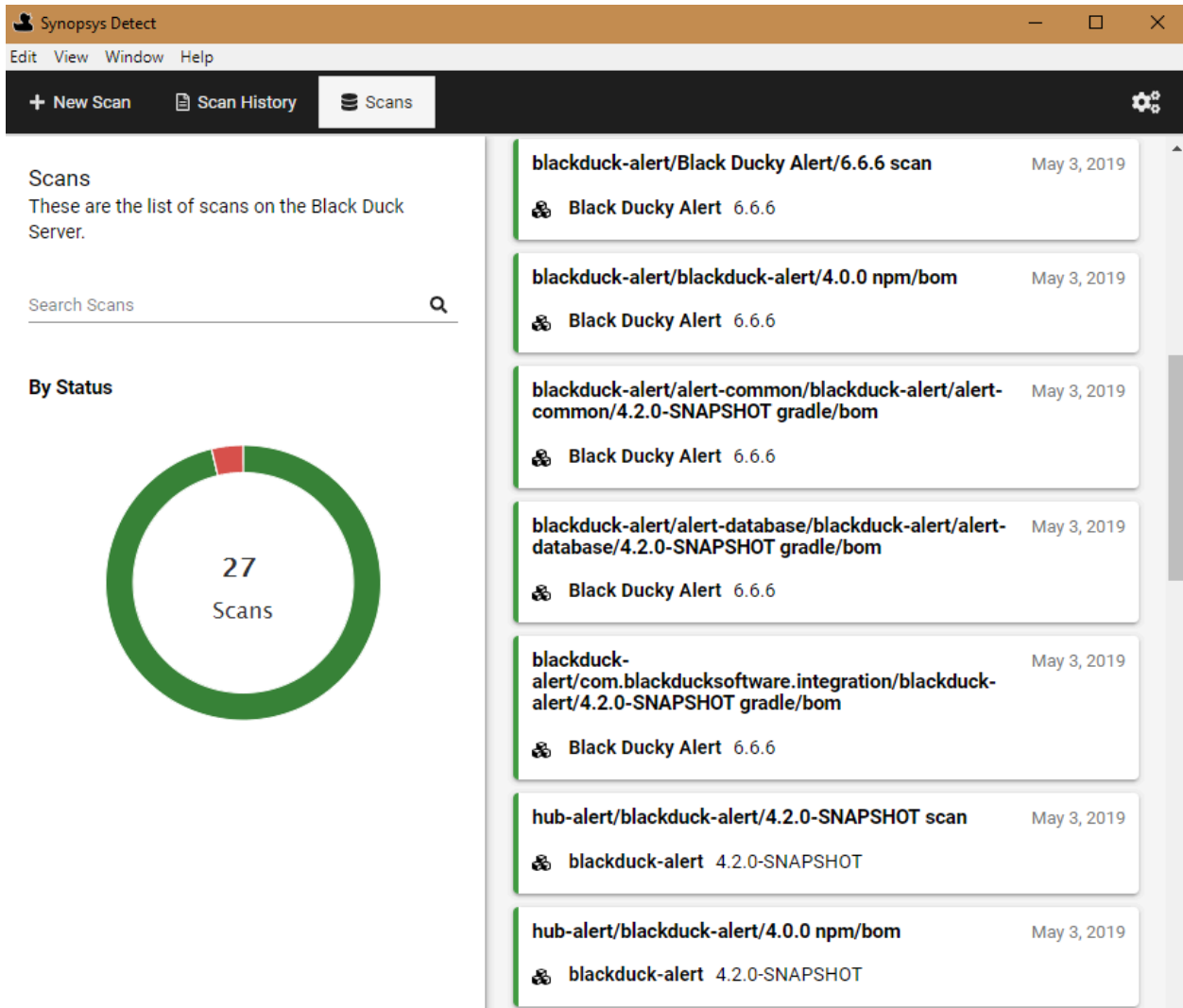
2. If the file is on your local system, you can drag and drop the scan file from your local machine to the **Scan History** tab.
3. Select the file to upload and click  in the upper right corner to display the file options.
4. Click **Upload Scan File to Black Duck**. The Upload Progress window appears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


3. Scanning your code • Using Black Duck Detect (Desktop)



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 Black Duck 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.

Projects or applications are limited to 10GB of Managed Code base.

 **Note:** If [SCM Integration](#) is enabled in your environment and you want to create a SCM project, see [Creating a SCM project](#).

To create a project:

1. Log in to Black Duck.
2. Click **+ Create Project** at the top of any page. If [SCM Integration](#) is enabled in your environment, select **Standard Project** from the menu. The **Project Details** page will display.

 **Create Project**

Project Details

Project Group
Black Duck Project Groups × ▼

Project Name *

SCM Repository

Description

Version Details

Version Name *

SCM Branch

License
Start typing to select a license... ▼

Phase *
In Planning ▼

Distribution *
External ▼

Cancel Save

3. 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 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, enter additional information such as:
 - **SCM Repository:** The URL of the source code management (SCM) repository where your code resides. This field is visible only if this feature is enabled in your environment. It can be manually edited or automatically populated by Detect after completing a package manager scan. Manually changing the SCM repository URL could break an existing scan if the URLs don't match. Note that this feature is available with Detect 8.x only.
 - **Description:** 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.
5. Type the version for this project in the **Version Name** field.
6. 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.
7. Click **Save**.
Black Duck displays the *Project Name* page.

Black Duck Project Groups
Sample Project

Project ★ Watching Project Versions: 2 Owner: System Administrator Overview Settings

Description
No description

Created
Nov 28, 2022 by sysadmin

Tags
No Tags

Custom Fields
No custom fields

Updated
Nov 28, 2022 by sysadmin

+ Create Version + Filter Filter versions...

Version	Phase	Last Updated	Last Scanned	License	Security Risk	License Risk	Operational Risk
1.0	In Planning	12:32 PM	Never	Unknown License			
1.1	In Planning	12:32 PM	Never	Unknown License			

Displaying 1-2 of 2

Mapping a scan to a project

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

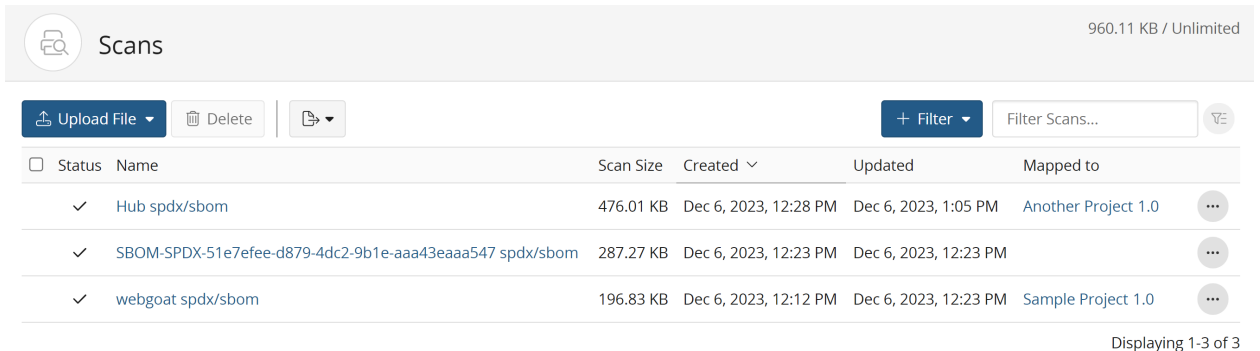
Note: You can scan a Docker image or file directory location or archive more than once, but you only have to map it to a project version once. The host and path may be changed, but as long as code location name is the same, Black Duck automatically updates the BOM of the project with any new information discovered during subsequent scans.

To map a scan to a project:

3. Scanning your code • Mapping a scan to a project

1. Log in to Black Duck.

2.  Click **Scans**.




Scans 960.11 KB / Unlimited

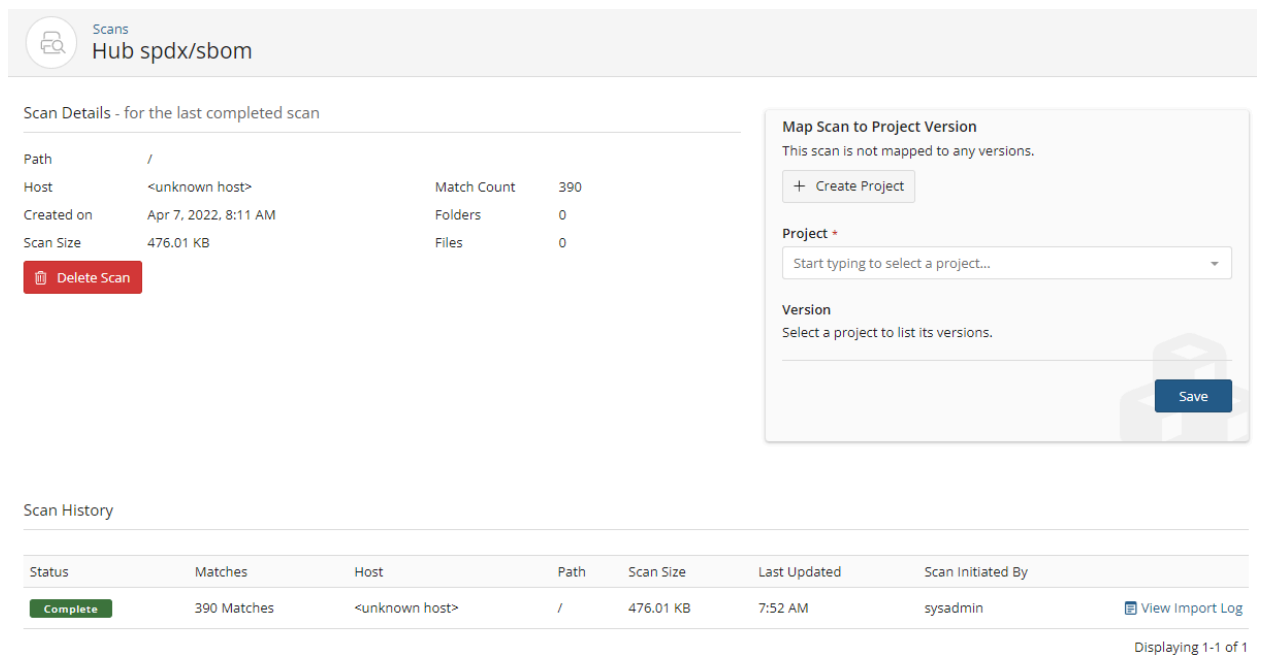
Upload File Delete + Filter Filter Scans...

Status	Name	Scan Size	Created	Updated	Mapped to
✓	Hub spdx/sbom	476.01 KB	Dec 6, 2023, 12:28 PM	Dec 6, 2023, 1:05 PM	Another Project 1.0
✓	SBOM-SPDX-51e7efee-d879-4dc2-9b1e-aaa43eaaa547 spdx/sbom	287.27 KB	Dec 6, 2023, 12:23 PM	Dec 6, 2023, 12:23 PM	
✓	webgoat spdx/sbom	196.83 KB	Dec 6, 2023, 12:12 PM	Dec 6, 2023, 12:23 PM	Sample Project 1.0

Displaying 1-3 of 3

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 Hub spdx/sbom

Scan Details - for the last completed scan

Path	/	Match Count	390
Host	<unknown host>	Folders	0
Created on	Apr 7, 2022, 8:11 AM	Files	0
Scan Size	476.01 KB		

Delete Scan

Map Scan to Project Version
This scan is not mapped to any versions.

+ Create Project

Project *
Start typing to select a project...

Version
Select a project to list its versions.

Save

Scan History

Status	Matches	Host	Path	Scan Size	Last Updated	Scan Initiated By
Complete	390 Matches	<unknown host>	/	476.01 KB	7:52 AM	sysadmin

View 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.

4. 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 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

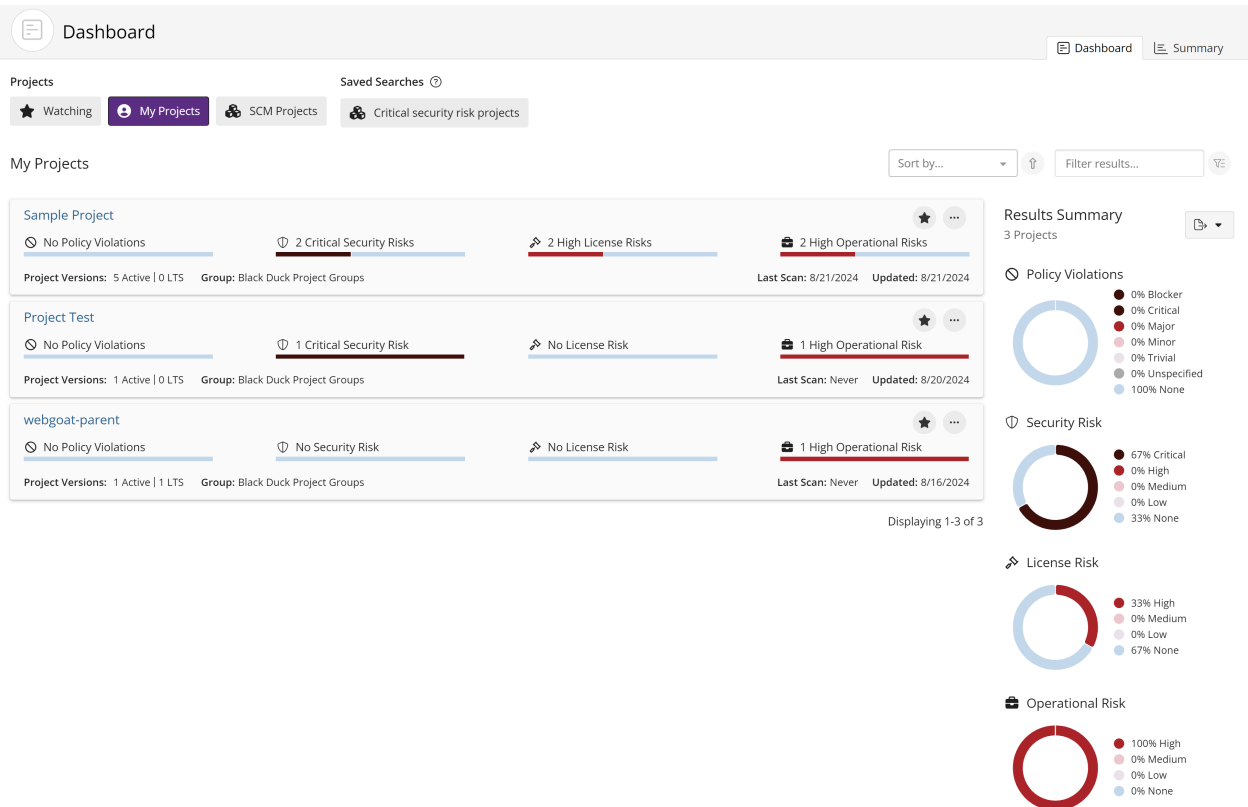
Note that the security risk values shown use CVSS v2 or CVSS v3.x scores, depending on which [security risk calculation you selected](#); by default, CVSS v3.x scores are shown. Note that the security risk graph displays a Critical risk category with a value of 0, if you selected CVSS v2.

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.

- 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.

Component - Apache Commons

Component Name	Version	License Risk
Apache Commons BeanUtils	> 1.9.4	No License Risk
Apache Commons Codec	> 1.13	No License Risk
Apache Commons Codec	> 1.15	No License Risk
Apache Commons Collections	> 3.2.2	No License Risk
Apache Commons Collections	> 4.1	No License Risk
Apache Commons Collections	> 4.4	No License Risk

Results Summary
42 Components

Security Risk

1% Critical
3% High
4% Medium
0% Low
92% None

License Risk

17% High
12% Medium
0% Low
71% None

Operational Risk

29% High
21% Medium
15% Low
35% None

- Create a saved [vulnerability search](#) to view the vulnerabilities that interest you.

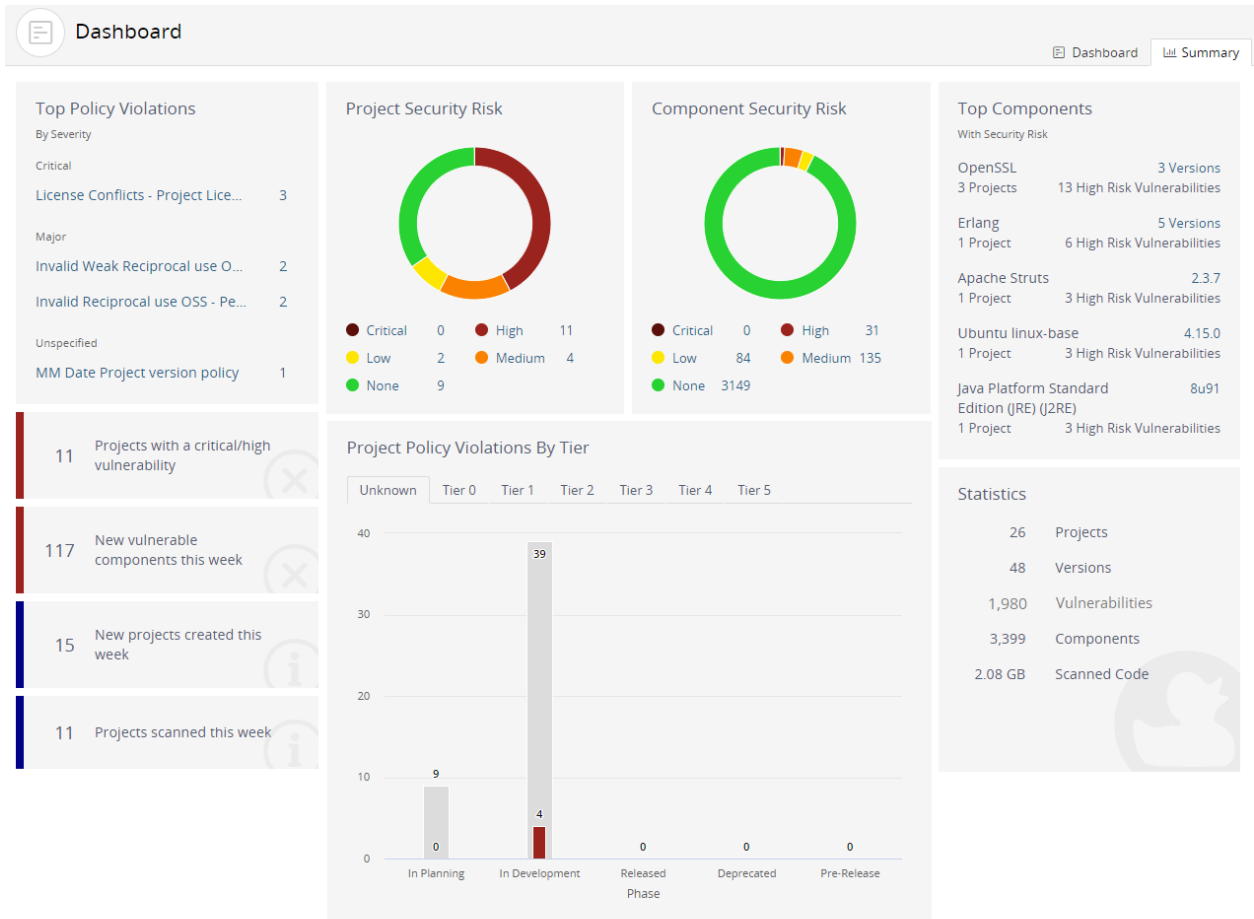
Vulnerability - Critical

Vulnerability ID	Overall Risk	Solution	Workaround	Exploit
BDSA-2015-0068	9.2 Critical	✓ Solution	No Workaround	Exploit CWE-79
BDSA-2015-0080	9.2 Critical	✓ Solution	No Workaround	Exploit CWE-79
BDSA-2010-0003	9.1 Critical	No Solution	No Workaround	No Exploit CWE-20, CWE-712
BDSA-2011-0017	9.2 Critical	✓ Solution	No Workaround	Exploit CWE-80

Results Summary
24,562 Vulnerabilities

- Use the [Summary Dashboard](#) to view the overall health of the projects you have permission to view and identify areas of concern.


4. Viewing risk in Black Duck • Project version pages



Note:

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

•

Click  or the logo in the upper left corner of the navigation bar to view the last dashboard (Dashboard or Summary) you viewed.

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

Phase: In Planning | Scans: Up to Date | 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 8
Medium 1
Low 0
None 7

Operational Risk
Number of Components

High 10
Medium 0
Low 0
None 4

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
Bit5Blog Bit 5 Blog 6.0	1 Match	Direct Dependency	Dynamically Linked	GPL-2.0+	High	High

- 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
Sample Project 1.0

Phase: In Planning | Scans: Up to Date | Status: Up to Date

Components Security Source Reports Details Settings

Security Risk
Number of Unique Component Origins

Critical 0 High 2 Medium 15 Low 8

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

Short Term Upgrade Recommendation
5.4.3.Final
2 Known Vulnerability

Long Term Upgrade Recommendation
6.1.2.Final
Has no known vulnerabilities

Identifier	Published	Overall Score	Status	CWE	Exploit	Workaround	Solution
BDSA 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

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, components, and vulnerabilities.

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.

4. Viewing risk in Black Duck • Viewing your dashboards

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, component versions, and vulnerabilities that are important to you: [search for projects](#), [components](#), and/or [vulnerabilities](#) and then [save the searches](#); use the Dashboard page to view the information from those saved searches.

Viewing dashboards



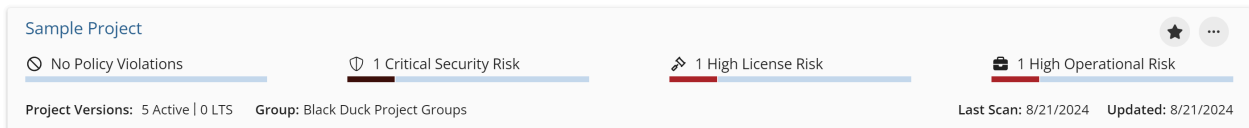
To view the dashboards, click **Dashboard**.

The dashboard page that appears depends on the last dashboard (a specific Dashboard page or [Summary Dashboard](#)) you viewed previously. 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 versions have Critical 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

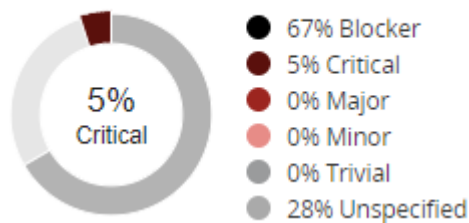


* Each project version is counted once by its highest severity risk

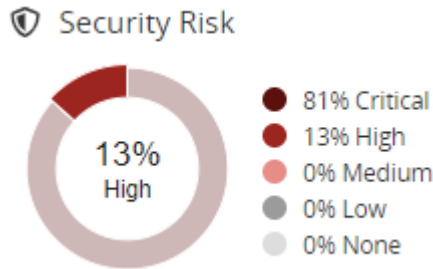
If a project version has risk, the version is only counted once and only its highest risk level is shown.



- 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:

Policy Violations



- 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 the project versions, component versions, and vulnerabilities that are important to you.

For each saved search, Black Duck lists the date and time this search was last updated.

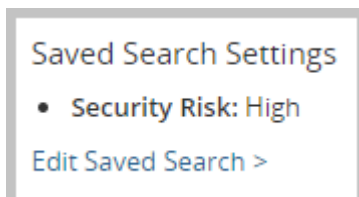
Results Summary

9 Components

Results updated at Feb 8, 2021 10:03 AM

 [Saved Search Settings](#)

Select **Saved Search Settings** to view the filters for this saved search.




Select **Edit Saved Search** to open the Find page displaying your saved search. Use the page to edit and save this revised saved search.

Project version saved searches

The screenshot shows a dashboard with a search bar containing 'sample'. Below the search bar, there are three project version cards for 'Sample Project A' (versions 1.0, 2.0, and 3.0). Each card displays risk metrics: Unspecified Policy Violations, Critical Security Risks, High License Risks, and High Operational Risks. To the right, there is a 'Results Summary' section with four donut charts: Policy Violations, Security Risk, License Risk, and Operational Risk. The Policy Violations chart shows 0% for all severity levels except 'Blocker' (0%). The Security Risk chart shows 34% Critical, 33% High, 0% Medium, 0% Low, and 33% None. The License Risk chart shows 67% High, 0% Medium, 0% Low, and 33% None. The Operational Risk chart shows 100% High, 0% Medium, 0% Low, and 0% None.


The following information is shown for each project version:

The detailed view shows a card for 'Sample Project > 1.0'. It features four risk metrics with progress bars: 'No Policy Violations', '8 Critical Security Risks', '1 High License Risk', and '149 High Operational Risks'. Below the metrics, it lists 'Group: Sample Project Gr...', '390 Components', 'Last Scan: 1/3/2024', 'Updated: 1/3/2024', 'License: Unknown License', and 'Phase: In Planning'.

-  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.

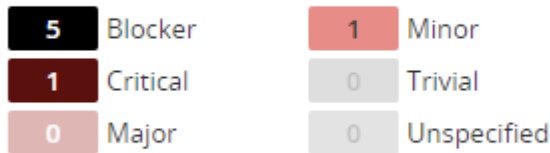
The close-up shows a bar with the text '5 Blocker Policy Violations'. The bar is filled with a dark red color, indicating the highest severity level.

 **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

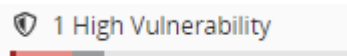


* Each component is counted once by its highest severity risk

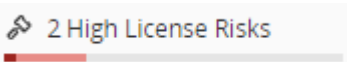
If a component has a policy violation, the component is only counted once and only its highest policy severity level is shown.

- 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.

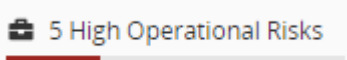
Security risk:



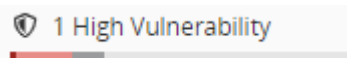
License risk:



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



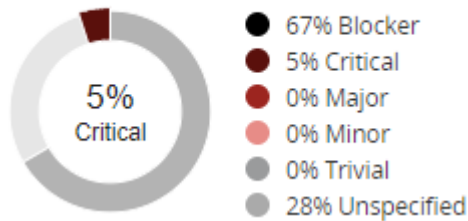
* Each component is counted once by its highest severity risk

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.

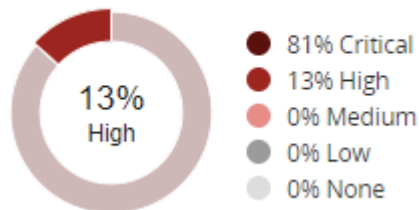
- Use the graphs to view overview information for all project versions in this dashboard categorized by policy severity and risk levels. The graphs lists the percentages for each level. You can also:
 - Hover over the graph to view the percentage of project versions with policy violations for each policy 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 shows a dashboard titled 'Component - Apache Commons'. It lists several components with their respective risk levels and usage statistics. On the right side, there are three donut charts: 'Security Risk' (1% Critical, 3% High, 4% Medium, 0% Low, 92% None), 'License Risk' (17% High, 12% Medium, 0% Low, 71% None), and 'Operational Risk' (29% High, 21% Medium, 15% Low, 35% None).

The following information is shown for each component.

This detailed view for 'Apache Struts 2.3.7' shows it is used by 9 project versions, has 4 critical policy violations, and no license risk. The overall risk level is 'High'. Other details include an unreviewed approval status, never first detected, released on 11/6/2012, 80 newer versions, and a last vulnerability on 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.

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

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

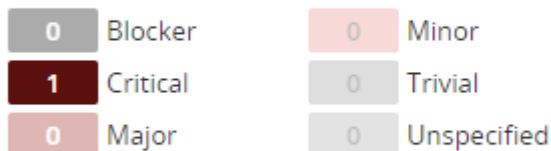
- Use the bar to quickly see the number of components with the highest policy severity level.

 1 Critical Policy Violation


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.

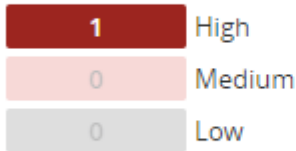
 1 High License Risk

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

4. Viewing risk in Black Duck • Viewing your dashboards

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).



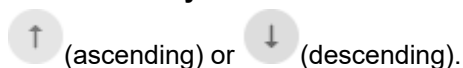
Select a value to display the **Security** tab of the Black Duck KB *Component Name Version* page, which lists the vulnerabilities associated with this version of this component.

A screenshot of the Black Duck KnowledgeBase interface. The page title is 'Apache Commons Collections > 3.2.1'. The 'Security' tab is selected. A table lists vulnerabilities with columns for Identifier, Published date, and Overall Score. The table shows four entries with scores ranging from 5.5 to 8.3. A search filter 'Filter Vulnerabilities...' is visible at the top right of the table area.

Identifier	Published	Overall Score
> BDSA BDSA-2015-0001 RCE	Apr 3, 2017	8.3 High
> BDSA BDSA-2015-0753 (CVE-2015-6420) RCE	May 3, 2019	8.3 High
> BDSA BDSA-2017-2285 (CVE-2017-15708) RCE	Dec 14, 2017	5.5 Medium
> BDSA BDSA-2015-0766 RCE	Aug 6, 2019	5.5 Medium

Displaying 1-4 of 4

- 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 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



- Use the filter field to filter the components shown in the dashboard.

Vulnerability saved searches

The screenshot shows a dashboard with a 'Vulnerability - Critical' filter. It displays a list of four vulnerabilities:

- BDSA-2015-0068**: Overall Risk 9.2 (Critical), Solution checked, No Workaround, Exploit (CWE-79).
- BDSA-2015-0080**: Overall Risk 9.2 (Critical), Solution checked, No Workaround, Exploit (CWE-79).
- BDSA-2010-0003**: Overall Risk 9.1 (Critical), No Solution, No Workaround, No Exploit (CWE-20, CWE-712).
- BDSA-2011-0017**: Overall Risk 9.2 (Critical), Solution checked, No Workaround, Exploit (CWE-80).

The following information is shown for each vulnerability:

The detailed view for BDSA-2020-1234 (CVE-2020-13430) shows:

- Used By**: 0 Project Versions
- Overall Risk**: 8.1 High
- Solution**: checked
- Workaround**: checked
- No Exploit**: CWE-79

- Select the vulnerability ID to view more information about the vulnerability, such as additional score values. You can view National Vulnerability Database (NVD) information by selecting the [CVE number](#) or view Black Duck Security Advisory (BDSA) information by selecting the [BDSA number](#).
- View the number of project versions that affected by this vulnerability next to **Used By**.

Used By | **2** Project Versions

Select **Project Versions** to open the **Affected Projects** tab for the vulnerability which lists the project versions affected by this vulnerability.

The 'Affected Projects' tab for BDSA-2014-0126 shows the following table:



Project	Component	Component Origin	Status	Target date	Actual date
cloudfoundry-identity-parent 3.6.3	Apache HttpClient 3.1	maven/commons-httpclient:commons-httpclient:3.1	New	Never	Never
cloudfoundry-identity-parent 3.6.3	Apache HttpClient 4.3.3	maven/org.apache.httpcomponents:httpclient:4.3.3	New	Never	Never
cloudfoundry-identity-parent 3.6.3	Apache HttpComponents Core 4.3.2	maven/org.apache.httpcomponents:httpcore:4.3.2	New	Never	Never
cloudfoundry-identity-parent 3.6.3	Apache HttpComponents Core 4.3.3	maven/org.apache.httpcomponents:httpcore:4.3.3	New	Never	Never

Displaying 1-4 of 4


- View the overall risk score. The search results show the Temporal Score for BDSA vulnerabilities, or the Base Score for NVD vulnerabilities and the associated risk level. Note that the score shown and risk level depends on the [selected security rankings](#).

4. Viewing risk in Black Duck • Viewing the health of your projects

Select the score to view individual scores: temporal, base, exploitability, and impact for BDSA; base, exploitability, and impact for NVD.

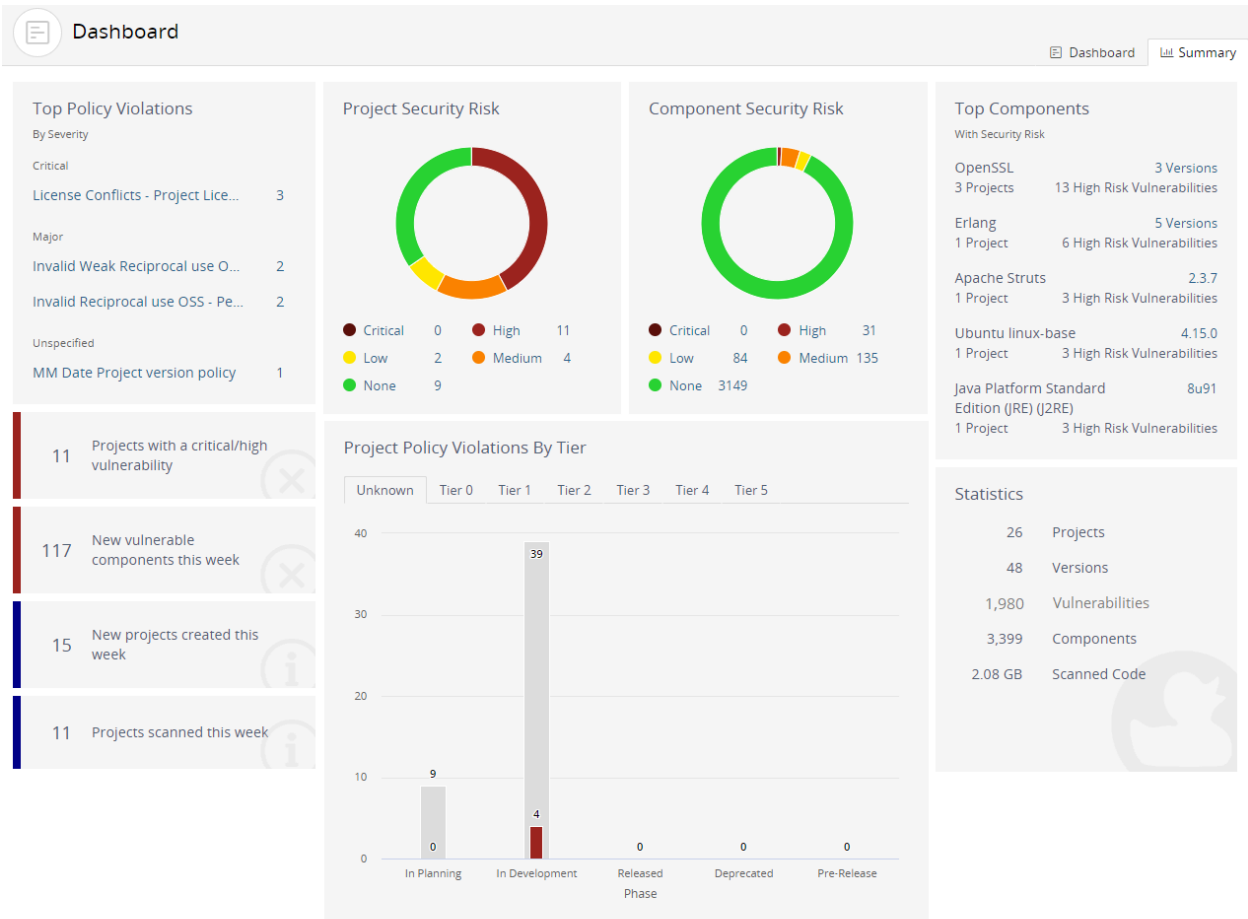
- View whether a solution, workaround, or exploit is available:
 -  indicates that there is a solution or workaround available for this vulnerability.
 -  indicates there is an exploit for this vulnerability.
- For each vulnerability, the search results also show:
 - First Detected.
 - Published date.
 - Last modified date.
 - Common Weakness Enumeration (CWE) number for this security vulnerability.

Exporting to CSV

You can export your Dashboard to CSV which converts the individual rows to tabular data. To do so, click the  button and select CSV.

Viewing the health of your projects

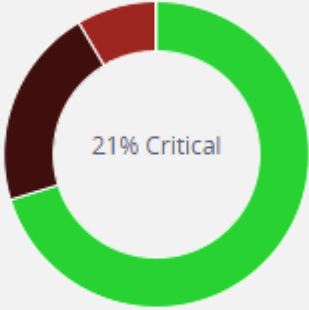
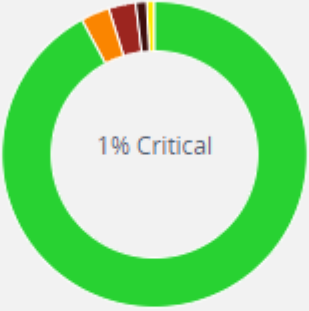
Use the **Summary** tab to view the overall health of your projects and identify areas of concern. The page consists of widgets that provide business critical information which you can use to quickly assess areas where you need to focus your attention.



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

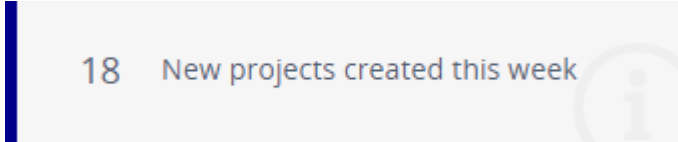
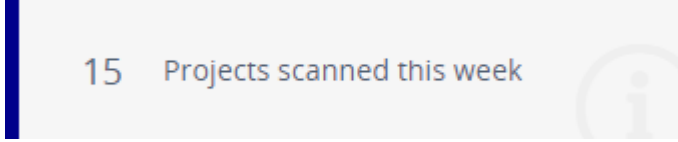
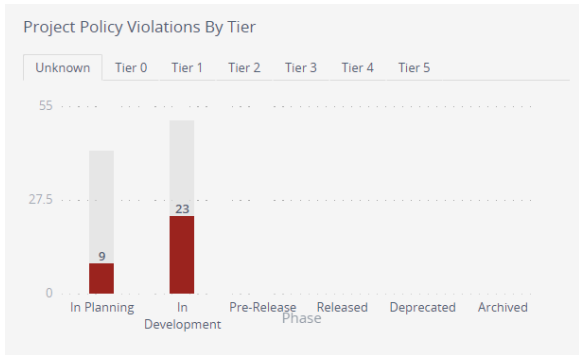
The following table describes each widget shown on the **Summary** tab and, where available, how to view additional information. Note that the security risk values shown use CVSS v2 or CVSS v3.x scores, depending on which [security risk calculation you selected](#); by default CVSS v3.x scores are shown.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

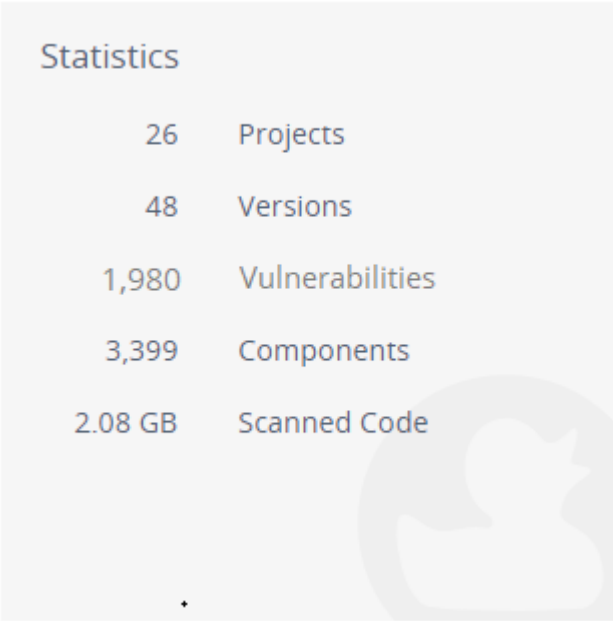
Widget	Description	More Information
<p>Top Policy Violations</p> <p>By Severity</p> <p>Major</p> <p>High Severity 10</p> <p>Medium Severity 10</p> <p>Major Rule 10</p> <p>Vulnerability Count 10</p> <p>Sample Rule 10</p>	<p>The Top Policy Violations widget displays up to the top five policy violations 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>	<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>
	<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. 	

Widget	Description	More Information												
<p data-bbox="250 289 570 323">Project Security Risk</p>  <table border="1" data-bbox="250 737 818 884"> <tr> <td>● Critical</td> <td>10</td> <td>● High</td> <td>4</td> </tr> <tr> <td>● Low</td> <td>0</td> <td>● Medium</td> <td>0</td> </tr> <tr> <td>● None</td> <td>33</td> <td></td> <td></td> </tr> </table>	● Critical	10	● High	4	● Low	0	● Medium	0	● None	33			<p data-bbox="906 247 1182 852">The Project Security Risk widget displays the number of projects you have permission to view for each level of security risk. 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 data-bbox="1187 247 1464 373">Hover over the graph to view the number of projects with that level of security risk.</p>
● Critical	10	● High	4											
● Low	0	● Medium	0											
● None	33													
<p data-bbox="250 974 646 1008">Component Security Risk</p>  <table border="1" data-bbox="250 1423 818 1570"> <tr> <td>● Critical</td> <td>29</td> <td>● High</td> <td>73</td> </tr> <tr> <td>● Low</td> <td>21</td> <td>● Medium</td> <td>77</td> </tr> <tr> <td>● None</td> <td>2331</td> <td></td> <td></td> </tr> </table>	● Critical	29	● High	73	● Low	21	● Medium	77	● None	2331			<p data-bbox="906 940 1182 1545">The Component Security Risk widget displays the number of components in projects you have permission to view for each security risk level. 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 data-bbox="1187 940 1464 1066">Hover over the graph to view the number of components with that level of security risk.</p>
● Critical	29	● High	73											
● Low	21	● Medium	77											
● None	2331													

4. Viewing risk in Black Duck • Viewing the health of your projects

Widget	Description	More Information																				
<p>Top Components With Security Risk</p> <table border="0"> <tr> <td>GNU C Library</td> <td>2.23</td> <td>1 Project</td> <td>5 Critical Risk Vulnerabilities</td> </tr> <tr> <td>Apache Struts</td> <td>2 Versions</td> <td>2 Projects</td> <td>3 Critical Risk Vulnerabilities</td> </tr> <tr> <td>Apache Camel</td> <td>2.15.1</td> <td>1 Project</td> <td>4 Critical Risk Vulnerabilities</td> </tr> <tr> <td>GnuTLS</td> <td>3.5.16</td> <td>1 Project</td> <td>1 High Risk Vulnerabilities</td> </tr> <tr> <td>zlib</td> <td>1.1.3</td> <td>1 Project</td> <td>1 High Risk Vulnerabilities</td> </tr> </table>	GNU C Library	2.23	1 Project	5 Critical Risk Vulnerabilities	Apache Struts	2 Versions	2 Projects	3 Critical Risk Vulnerabilities	Apache Camel	2.15.1	1 Project	4 Critical Risk Vulnerabilities	GnuTLS	3.5.16	1 Project	1 High Risk Vulnerabilities	zlib	1.1.3	1 Project	1 High Risk Vulnerabilities	<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 or number of versions to view the Component Version Details page.</p>
GNU C Library	2.23	1 Project	5 Critical Risk Vulnerabilities																			
Apache Struts	2 Versions	2 Projects	3 Critical Risk Vulnerabilities																			
Apache Camel	2.15.1	1 Project	4 Critical Risk Vulnerabilities																			
GnuTLS	3.5.16	1 Project	1 High Risk Vulnerabilities																			
zlib	1.1.3	1 Project	1 High Risk Vulnerabilities																			
<p>30 Projects with a critical/high vulnerability</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>																				
<p>80 New vulnerable components this week</p>	<p>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.</p>	<p>N/A.</p>																				

Widget	Description	More Information
 <p>18 New projects created this week</p>	<p>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.</p>	<p>N/A.</p>
 <p>15 Projects scanned this week</p>	<p>The Projects scanned this week widget displays the number of projects with scans from the past seven days, including today.</p>	<p>N/A.</p>
 <p>Project Policy Violations By Tier</p> <p>Unknown Tier 0 Tier 1 Tier 2 Tier 3 Tier 4 Tier 5</p> <p>9 23</p> <p>In Planning In Development Pre-Release Phase Released Deprecated Archived</p>	<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. 	<p>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>

Widget	Description	More Information
	<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</i> ignored components. • Scanned Code lists the number of GBs scanned for all scans. 	N/A.

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. Note that Black Duck displays the numbers together in reports and in the UI because they represent the same vulnerability from different sources.

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 v3.x scores.

- CVSS v2 scores have 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 have 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.

Estimated Security Risk

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

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

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

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

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 ranking](#).

Note that the security ranking also defines how vulnerabilities appear in reports. Depending on the data available, the vulnerability will be presented as either: BDSA (NVD) or NVD (BDSA). For example, if the security ranking is NVD2, BDSA2, BDSA3, NVD3 then:

- Vulnerability A has data for just NVD3. The vulnerability is listed as NVD-1234-5678 in the report.
 - Vulnerability B has data for NVD3 and BDSA3. The report lists it as BDSA (NVD).
 - Vulnerability C has data for everything. The report lists it as NVD (BDSA).
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 Dashboard pages for a high-level overview of risk:
 - [Use the Watched or My Project dashboards](#) to view the security risk across all your projects.
 - [Create saved searches](#) to customize the information shown on the Dashboard page to view the projects, components, and vulnerabilities that interest you.
 - 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.

5. 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 the BOM.

The screenshot shows the Black Duck Project Groups interface for 'Sample Project' 1.0.0. The 'Components' tab is active, displaying a BOM. At the top, there are three risk charts: Security Risk (4 Critical, 3 High, 4 Medium, 0 Low, 17 None), License Risk (6 High, 2 Medium, 0 Low, 20 None), and Operational Risk (24 High, 3 Medium, 0 Low, 1 None). Below these charts are filters for Snippets (78 Unconfirmed) and Unmatched Components (1 Unmatched). The main table lists components with columns for Component, Source, Match Type, Match Score, Usage, License, Security Risk, and Operational Risk. The table shows four components: AOP Alliance (Java/J2EE AOP standard) 1.0, Apache Commons DBCP 1.2.2, Apache Commons FileUpload 1.3.3, and Apache Commons IO 2.2. Each component has a '1 Match' source, a '100%' match score, and is 'Dynamically Linked'. The license for all is 'Apache-2.0'. The Security Risk for the first three is 'None' and for the last is '1'. The Operational Risk for all is 'High'.

Component	Source	Match Type	Match Score	Usage	License	Security Risk	Operational Risk
AOP Alliance (Java/J2EE AOP standard) 1.0	1 Match	Transitive Dependency	100%	Dynamically Linked	Public Domain	None	High
Apache Commons DBCP 1.2.2	1 Match	Direct Dependency	100%	Dynamically Linked	Apache-2.0	None	High
Apache Commons FileUpload 1.3.3	1 Match	Direct Dependency	100%	Dynamically Linked	Apache-2.0	1	High
Apache Commons IO 2.2	1 Match	Transitive Dependency	100%	Dynamically Linked	Apache-2.0	1	High

By default, the BOM displays a "flat" view of components where all components found are listed at the same level.

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 Black Duck KB, you may be using a version of the component that is not available in 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 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 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.

5. Viewing your BOM • Adjusting the component and/or component version in a BOM

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.

Black Duck Project Groups
Sample Project 1.0.0

Project Phase: In Development Scans: Up to Date Status: Up to Date Last Updated: 10:21 AM

Components Security Source Reports Details Legal Settings

Security Risk
Number of Components
Critical 4
High 3
Medium 4
Low 0
None 17

License Risk
Number of Components
High 6
Medium 2
Low 0
None 20

Operational Risk
Number of Components
High 24
Medium 3
Low 0
None 1

Snippets
78 Unconfirmed
Unmatched Components
1 Unmatched

Print Add Bulk Actions Compare to... Ignore Not Ignored Snippet Match Status Confirmed Match Ignore Not Ignored Filter

Component	Source	Match Type	Match Score	Usage	License	Security Risk	Operational Risk
AOP Alliance (Java/J2EE AOP standard) 1.0	1 Match	Transitive Dependency	100%	Dynamically Linked	Public Domain	High	High
Apache Commons DBCP 1.2.2	1 Match	Direct Dependency	100%	Dynamically Linked	Apache-2.0	High	High
Apache Commons FileUpload 1.3.3	1 Match	Direct Dependency	100%	Dynamically Linked	Apache-2.0	1	High
Apache Commons IO 2.2	1 Match	Transitive Dependency	100%	Dynamically Linked	Apache-2.0	1	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 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:

Print Add Bulk Actions Compare to... Ignore Not Ignored Snippet Match Status Confirmed Match Ignore Not Ignored Filter

Component	Source	Match Type	Match Score	Usage	License	Security Risk	Operational Risk
Apache Commons Collections ?	1 Match	Direct Dependency	100%	Dynamically Linked	Apache-2.0	1 3	High

Displaying 1-1 of 1