BLACKDUCK

BY SYNOPSYS®

Getting Started

Version 2019.4.3

This edition of the *Getting Started* refers to version 2019.4.3 of Black Duck.

This document created or updated on Wednesday, May 15, 2019.

Please send your comments and suggestions to:

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

Contents

Black Duck documentation

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

Title	File	Description
Release Notes	release_notes.pdf	Contains information about the new and improved features, resolved issues, and known issues in the current and previous releases.
Installing Black Duck using Docker Compose	install_compose.pdf	Contains information about installing and upgrading Black Duck using Docker Compose.
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.

Title	File	Description
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.

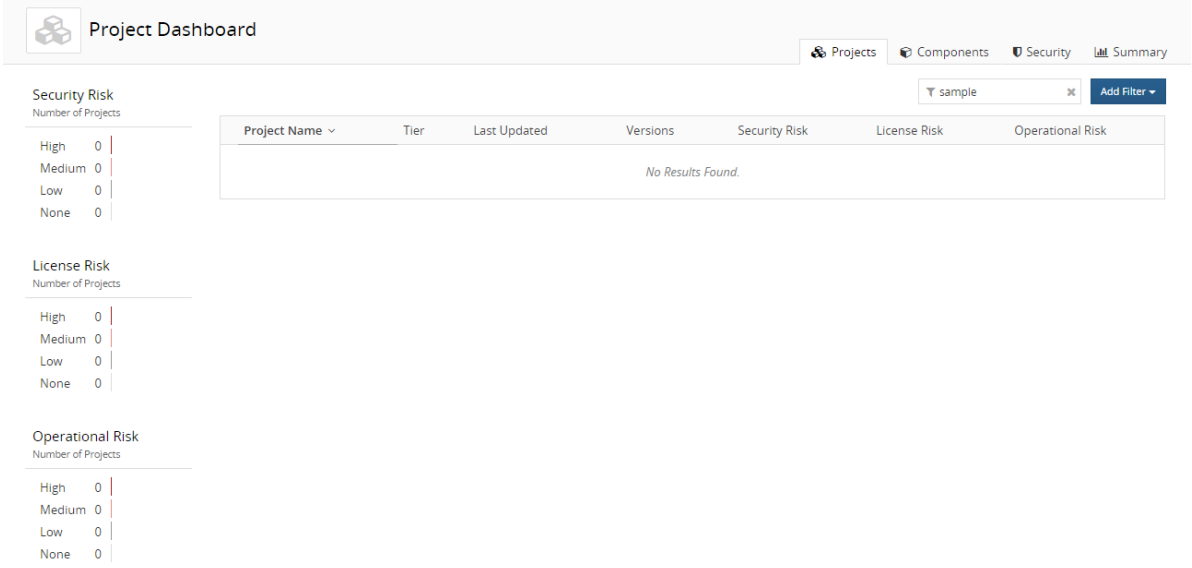
To log in to Black Duck

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 log in, Black Duck displays your Dashboard page.



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.

Chapter 2: 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.

Tip: **Want to Learn More?** Check out the Black Duck: Using the Scanner course on Black Duck Academy. You will learn how to use both the Black Duck Scanner and CI plug-ins to generate an inventory of open source components found in your application along with a mapping to known open source vulnerabilities associated with those components.

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.

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**.

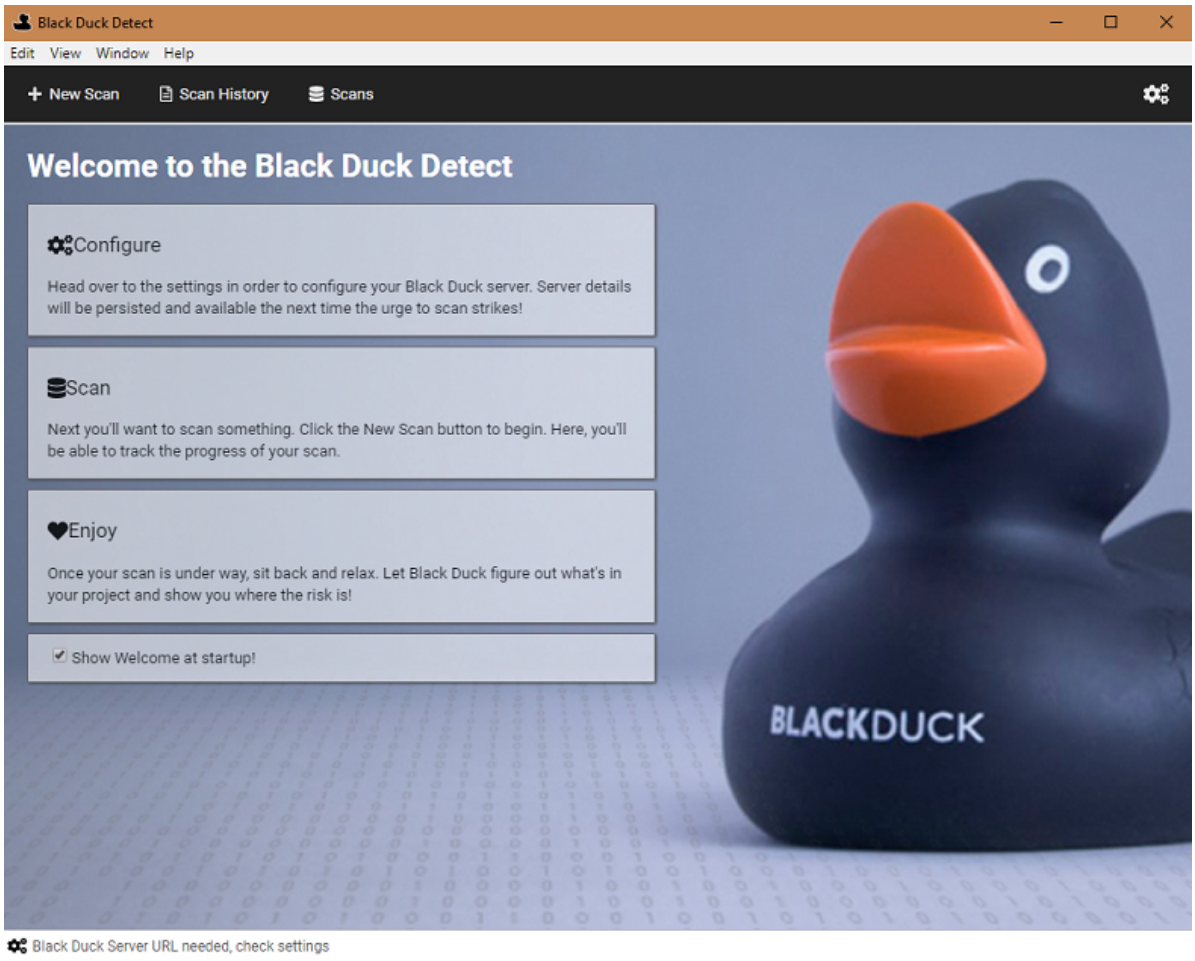
3. Select the operating system you wish to use in the **Downloads Synopsys Detect (Desktop)** section to download the executable from Google Cloud Storage.

4. Run the executable to install Black Duck Detect Desktop.

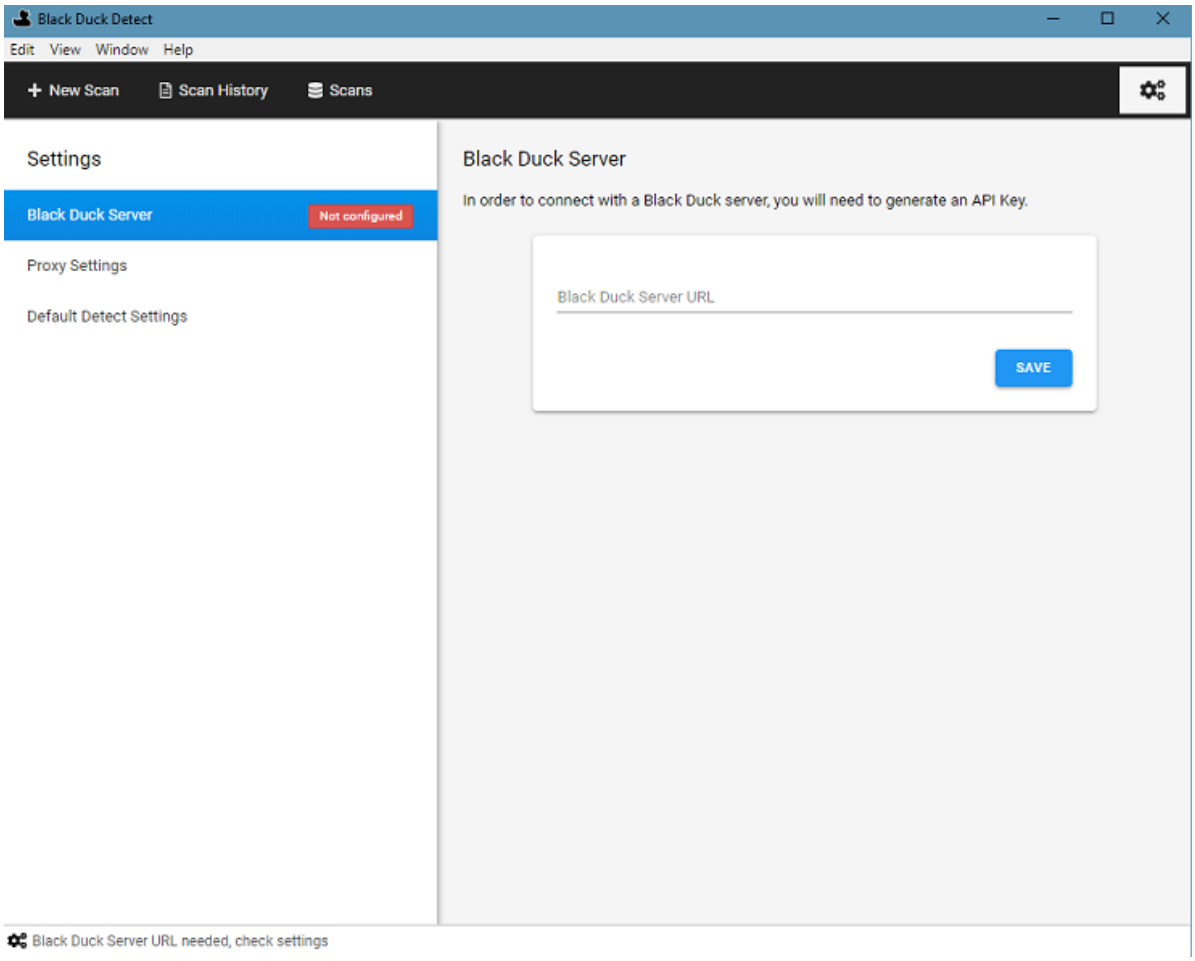
Configuring Black Duck Detect Desktop

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

1. After installing Black Duck 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

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**. Black Duck Detect Desktop connects to the Black Duck server and displays the version of Black Duck you are connected to.

3. Generate an API key (user access token).
    a. Enter a key name (optional), your username, and password.
    b. Click **Generate**.

> **Note:** You must create an API key from Black Duck Detect Desktop to use Black Duck Detect Desktop

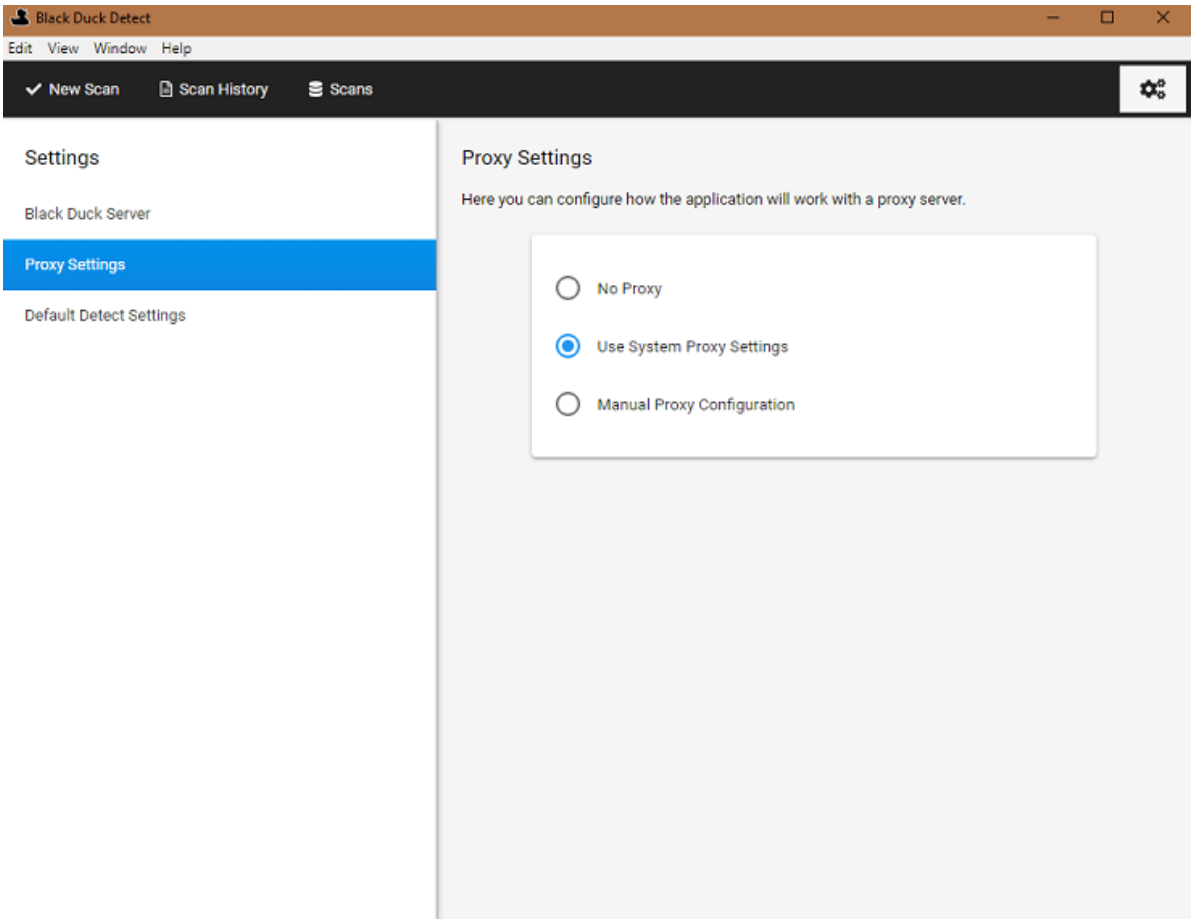
Proxy settings

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

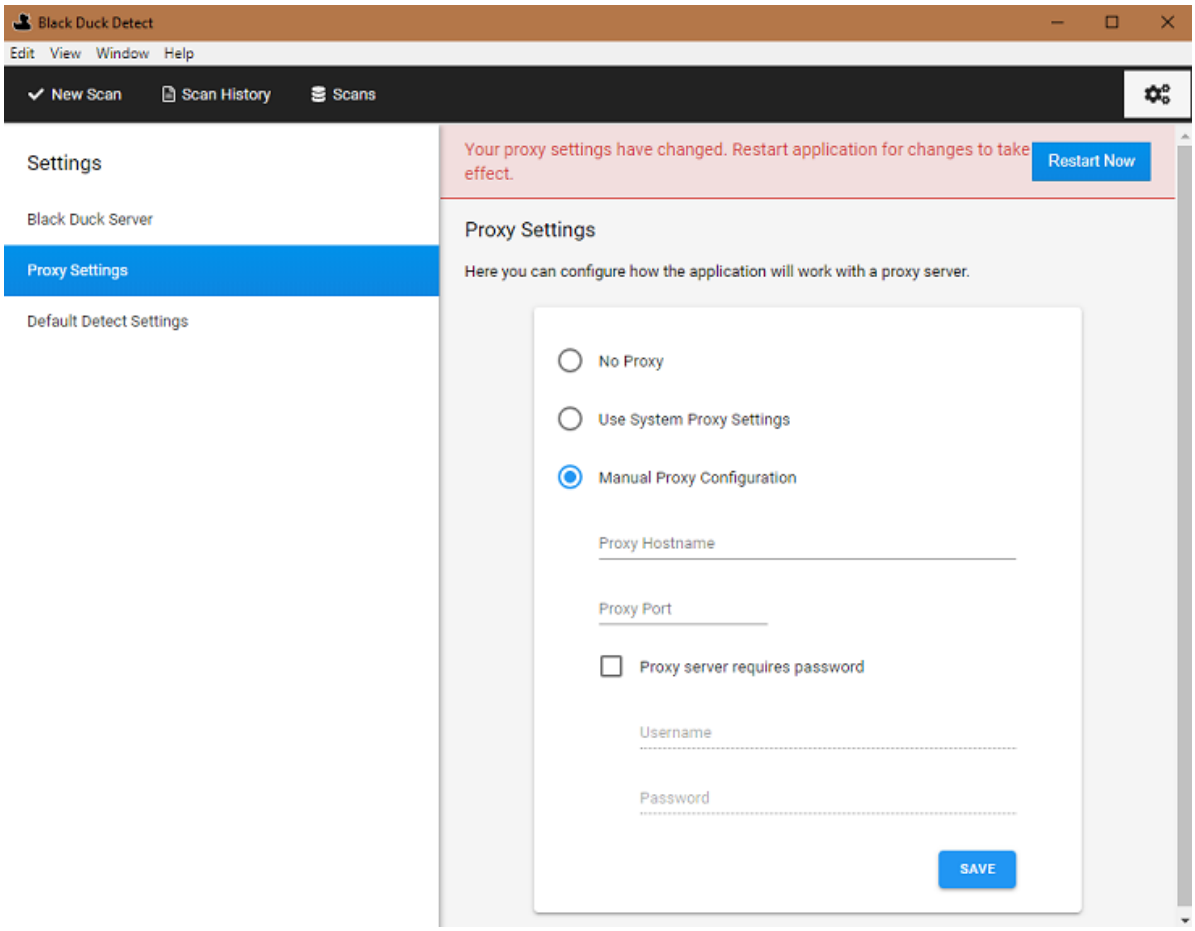
If you are required to manually enter your proxy settings or you do not require a proxy, you can modify these default settings.

To modify the default proxy settings

1. 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.

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 sever 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 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.

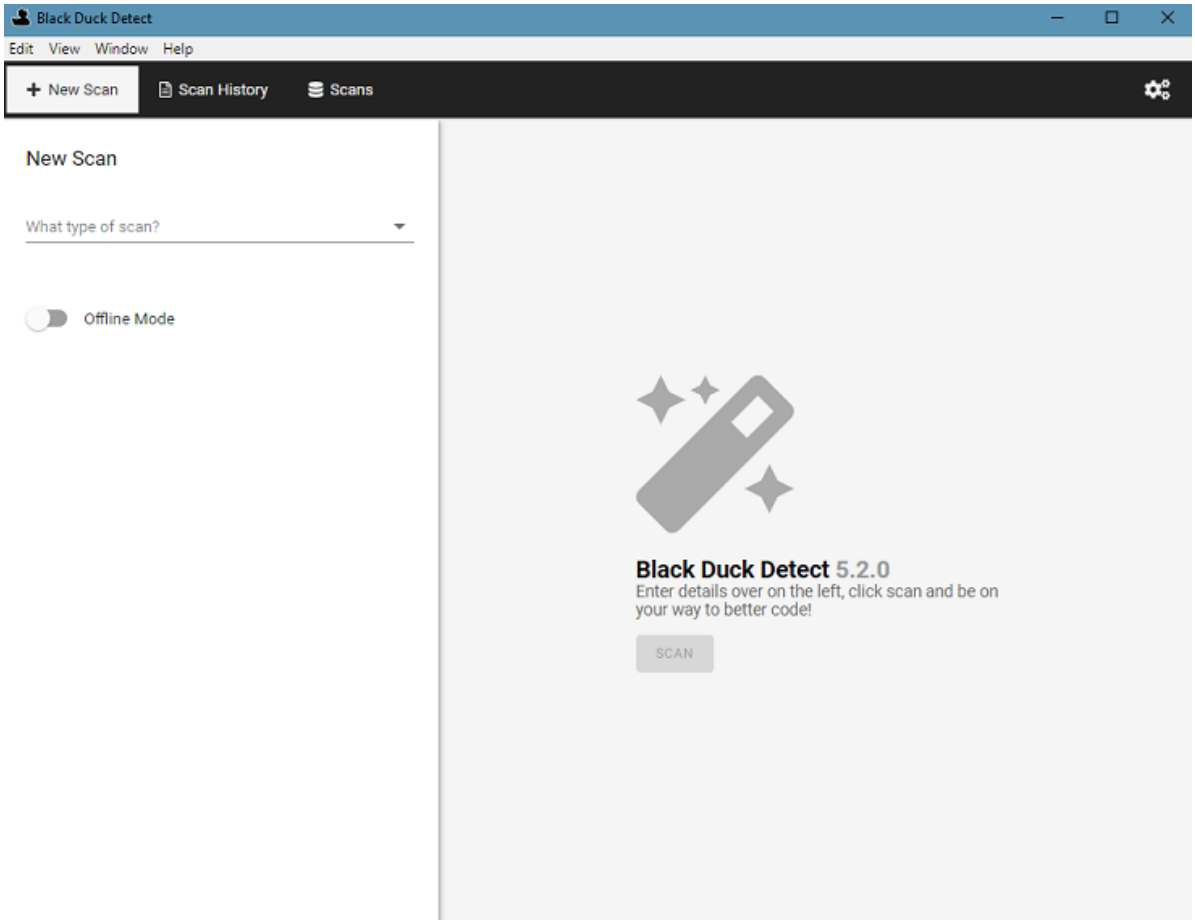
To specify project and/or version names:

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.

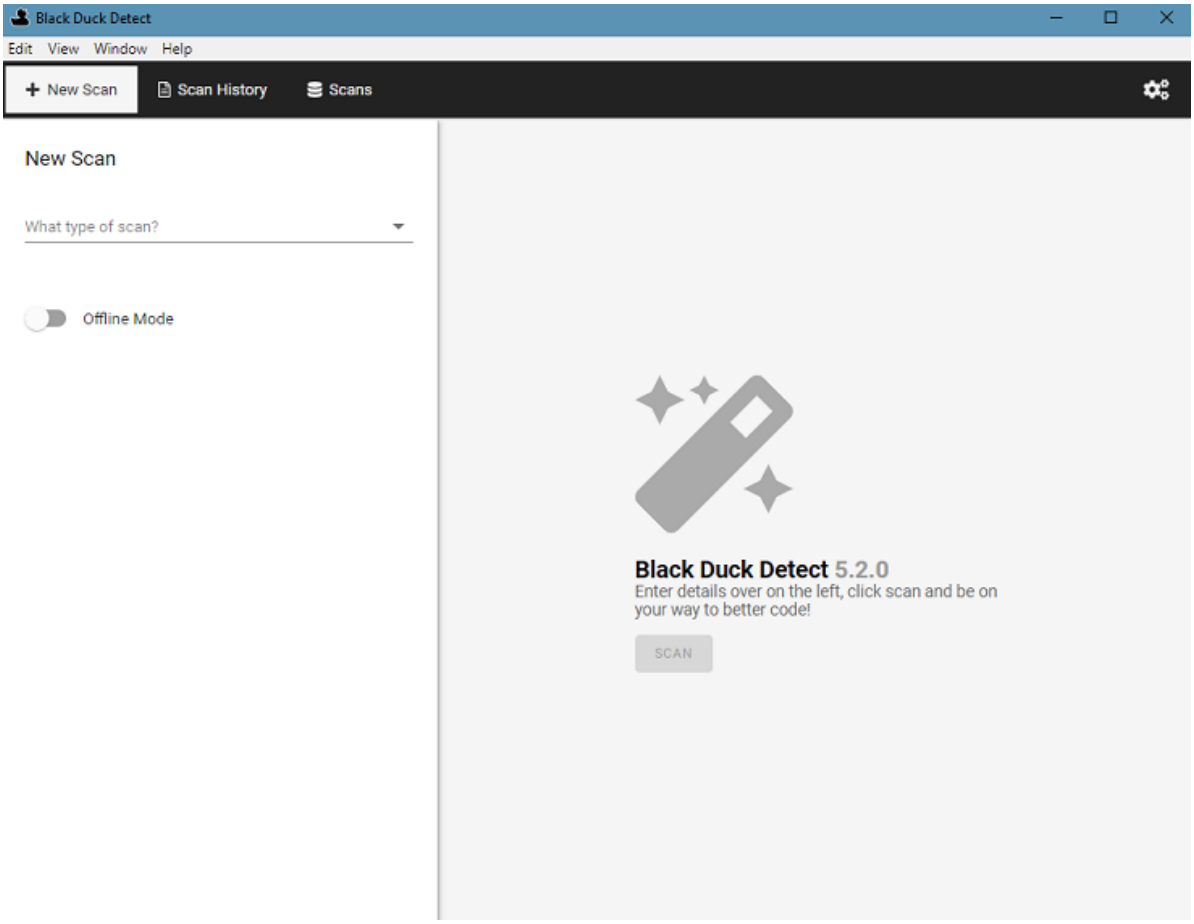
   If you have purchased a snippet scanning license and want to enable snippet scanning, select **Snippet Scanning** from the **Settings** options and enable it.
5. Click **Scan**.

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

Scanning binary/executable

To scan a single binary or executable

1. Click **New Scan**.



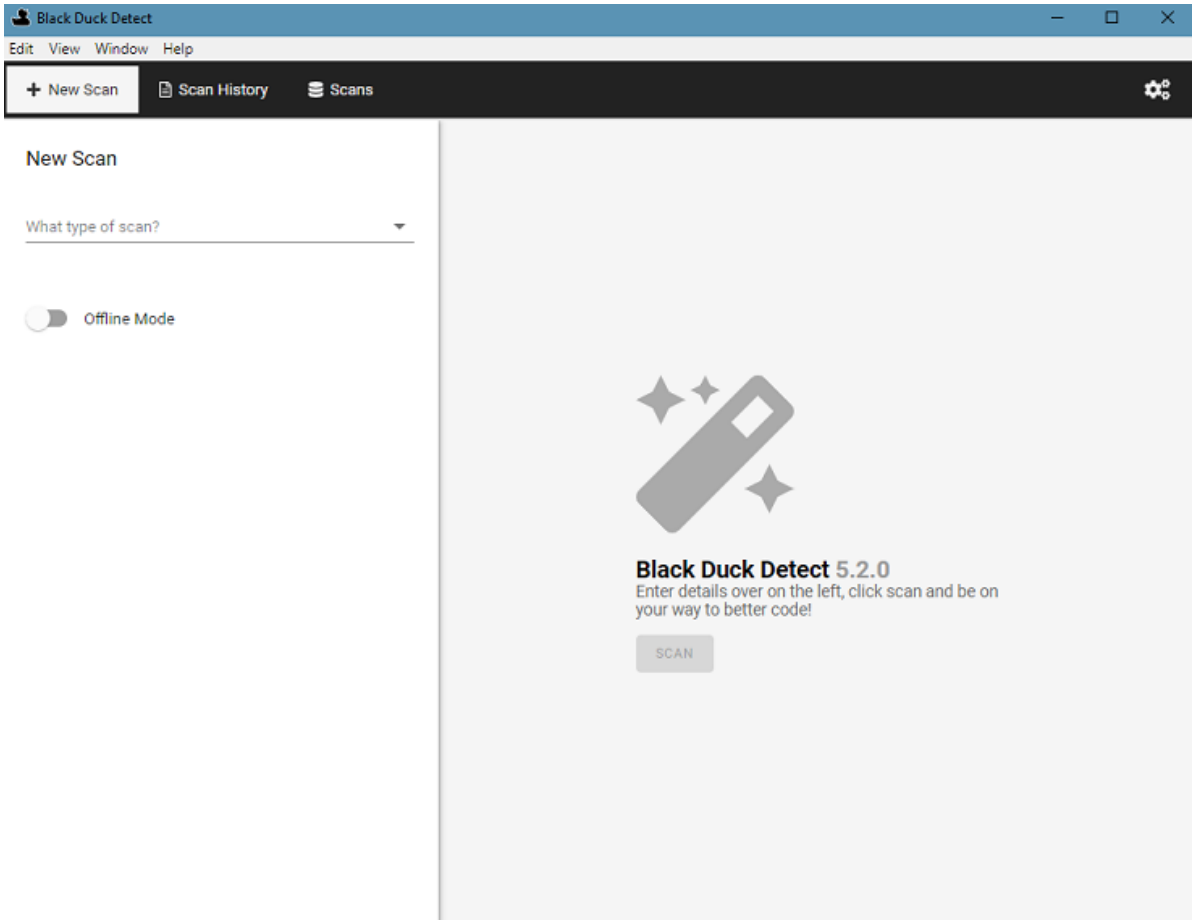
2. From the **What type of scan?** list, select **Binary/Executable**,
3. Click to select the binary or executable you would like to scan.
4. Optionally, modify or configure any project settings by clicking **ADD** and selecting the setting.
5. Click **Scan**.

   The status of the scan appears along with an option to cancel the scan.
6. When the scan is complete, select the **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:
   - Enter the Docker image name.
   - Select **Choose Docker File (.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 **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.

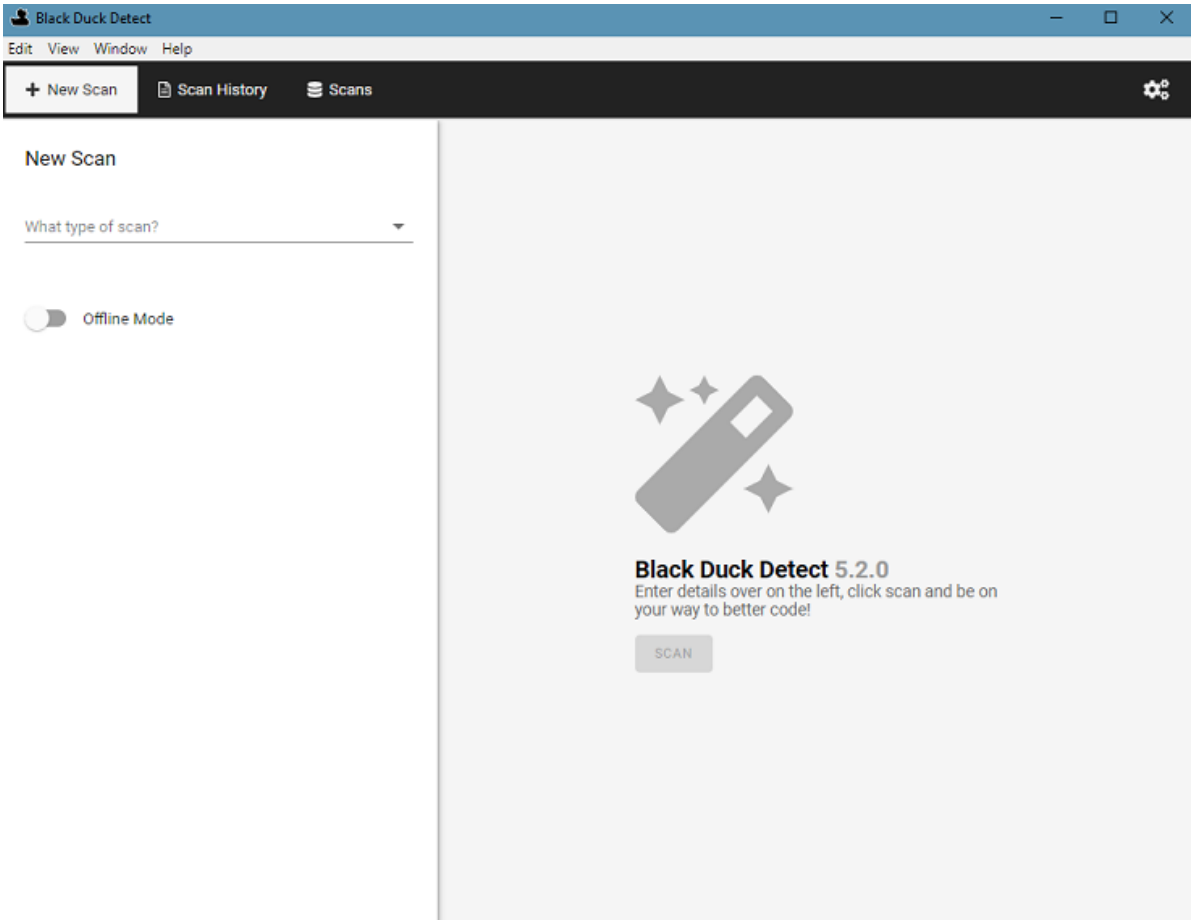
Creating a scan file

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 **Scan History** tab to view information on the completed scan.

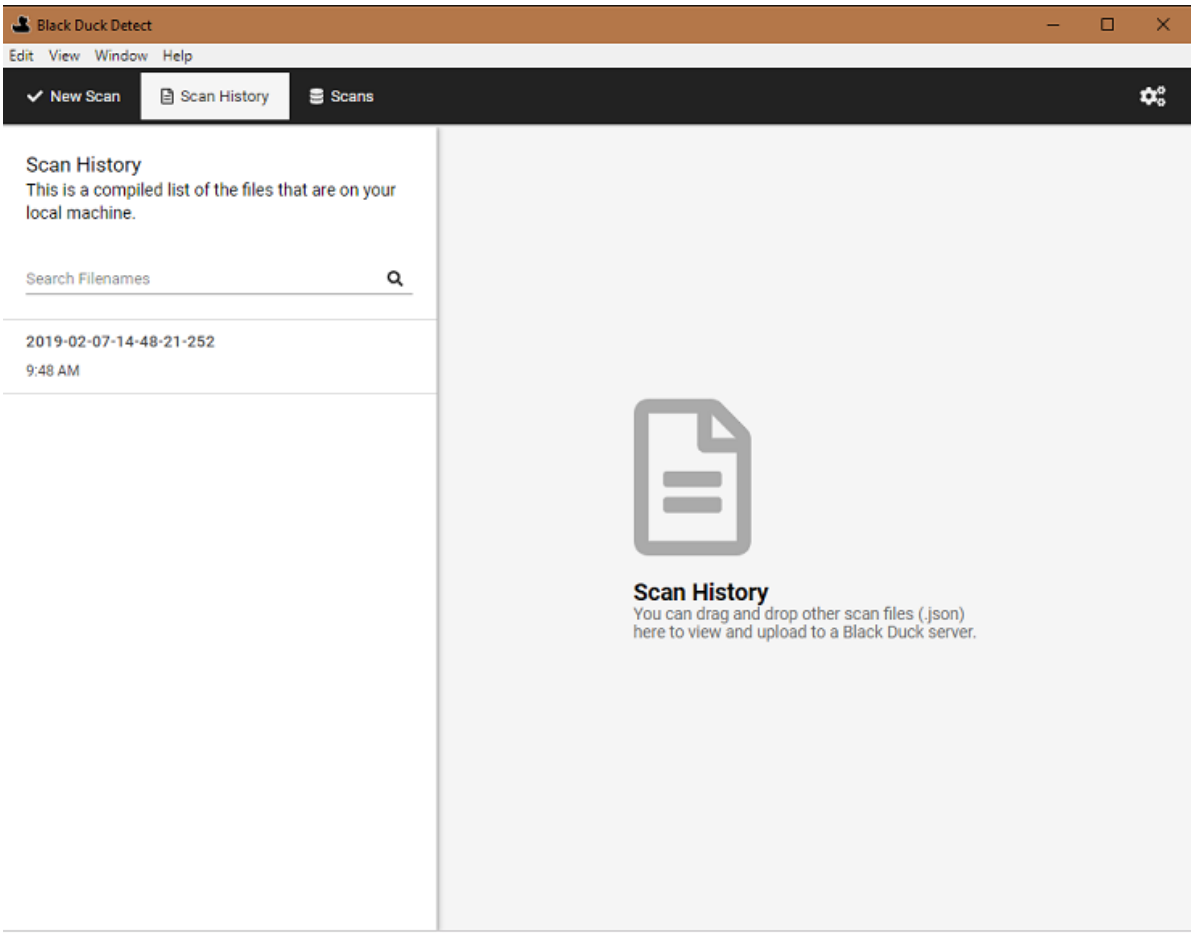
Managing scans

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

1. Click **Scan History**.

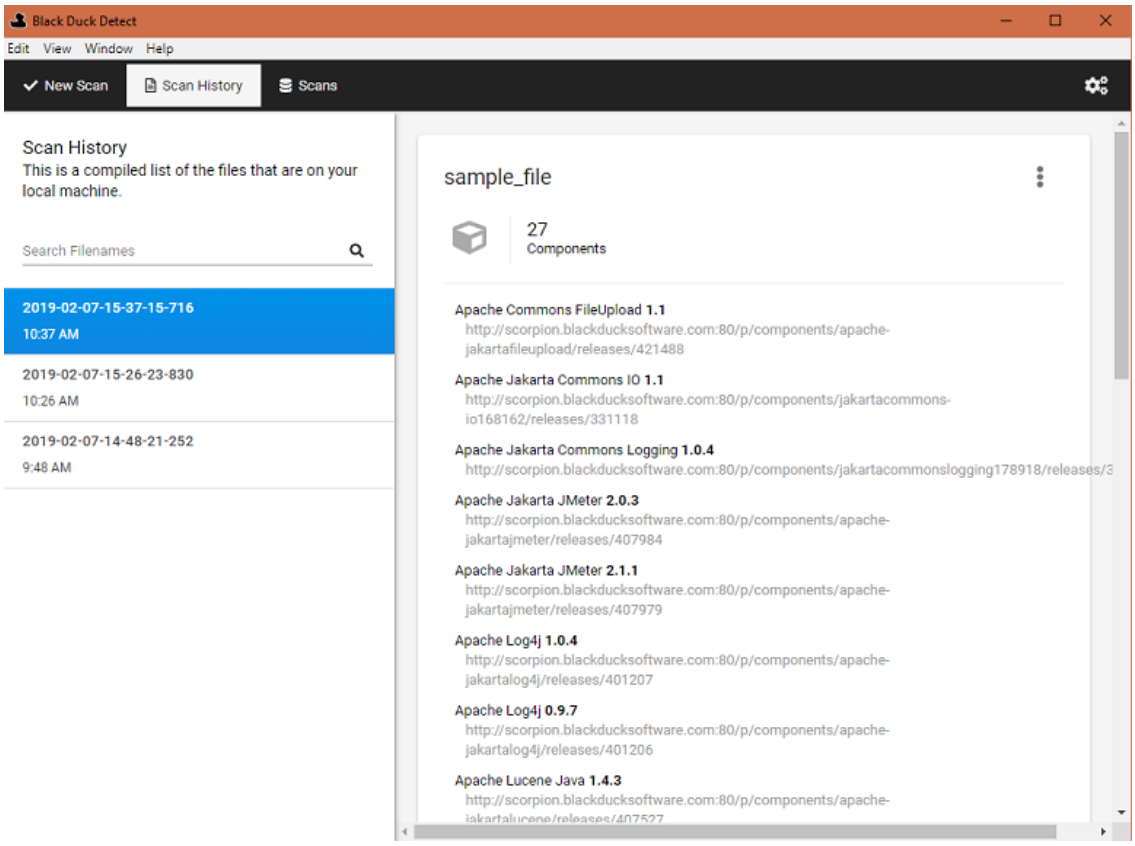
   A list of scans on your local system appears in the left column of the tab.

   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:

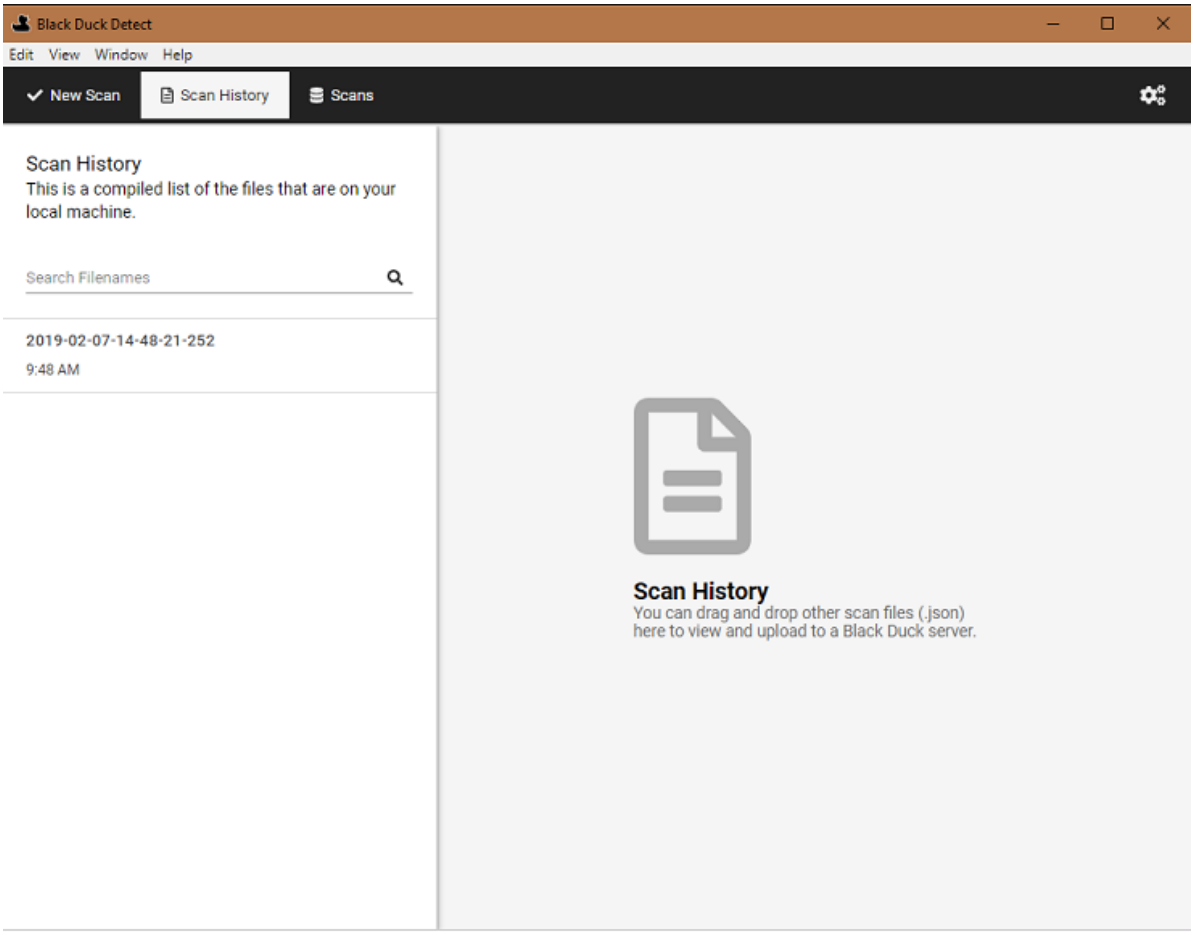


- View the location of the file on your system by clicking  and selecting **Show File**.
- Upload the file, as described in the next section.
- Delete the scan by hovering over the scan name in the left column and clicking **Delete**. Click **Yes** to confirm.

Uploading scan files to Black Duck

You can use Black Duck 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.

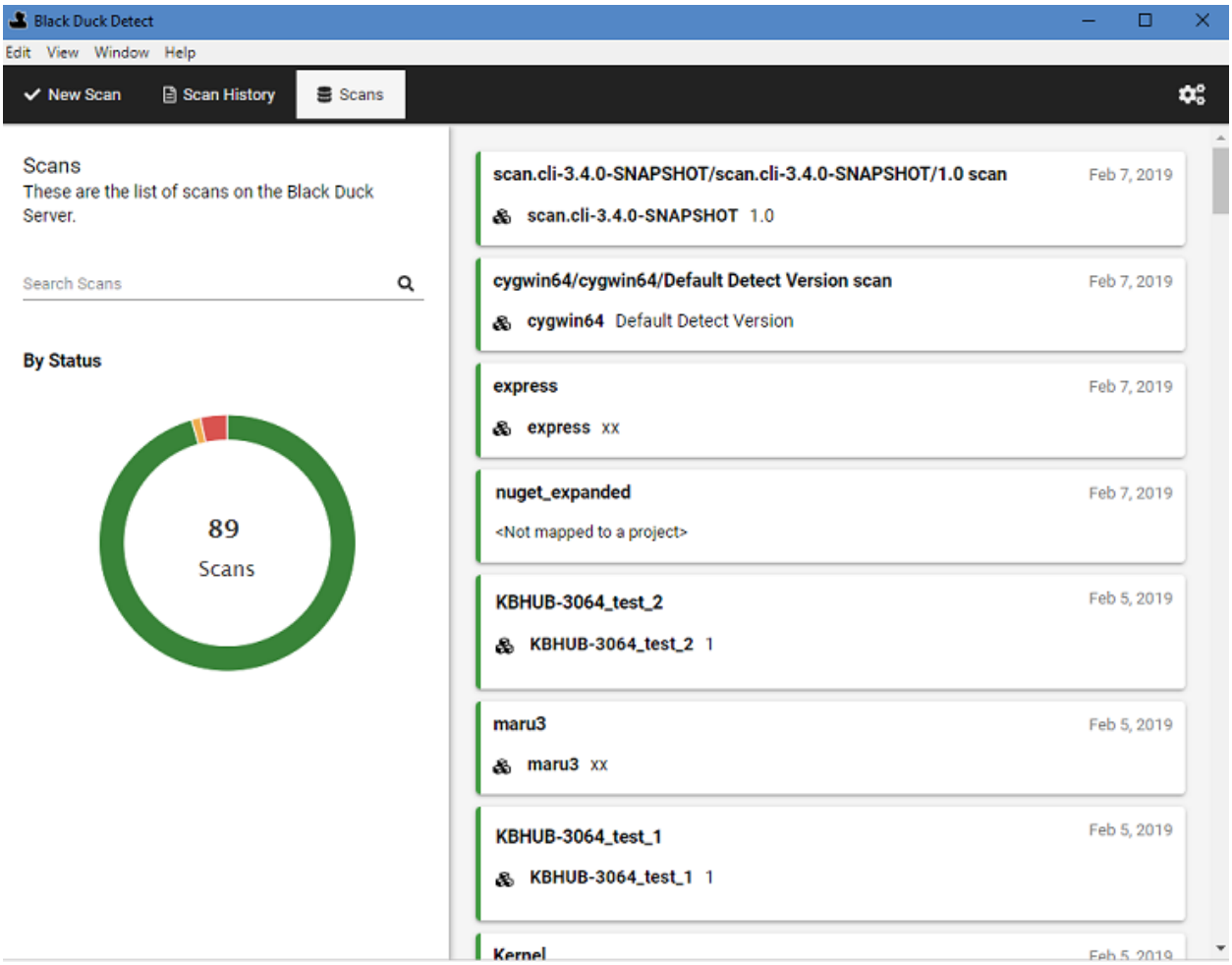
3. Select the file to upload and click ⋮ in the upper right corner to display the file options.

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 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

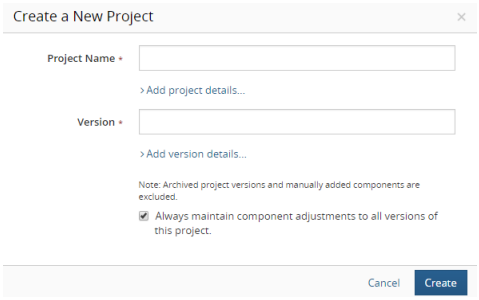
A project is the base unit in Black Duck. A project can be both a stand-alone development project and part of another project. For example, Apache Tomcat is a project in its own right but it may also be part of other, larger projects. You must create the projects that you want to make available for search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

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

Tip: **Want to Learn More?** Check out the Black Duck: Creating Projects course at Synopsys Software Integrity, Customer Education. You will learn how to create and save a Black Duck project as well as how to change overall project settings.

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.

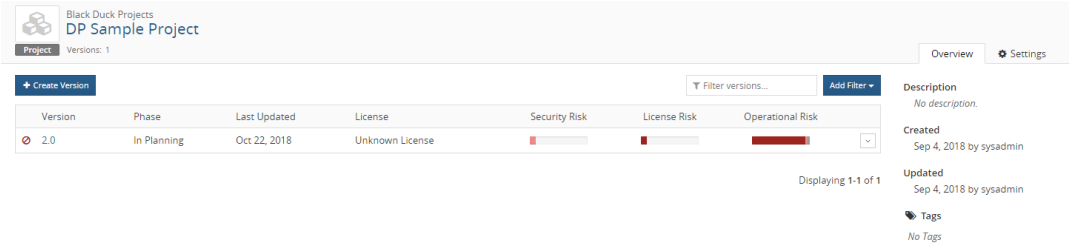
Note: If the user you add is not already a project member, Black Duck adds the user to the project team.

- 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.



Mapping a scan to a project

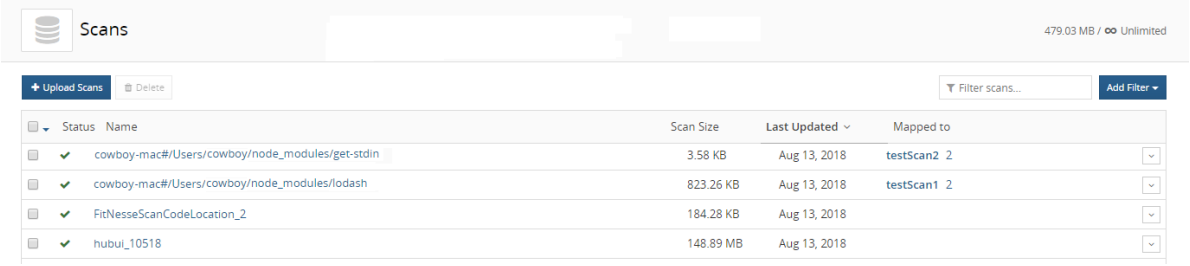
Mapping a scan adds the scan data to the BOM of a project version.

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

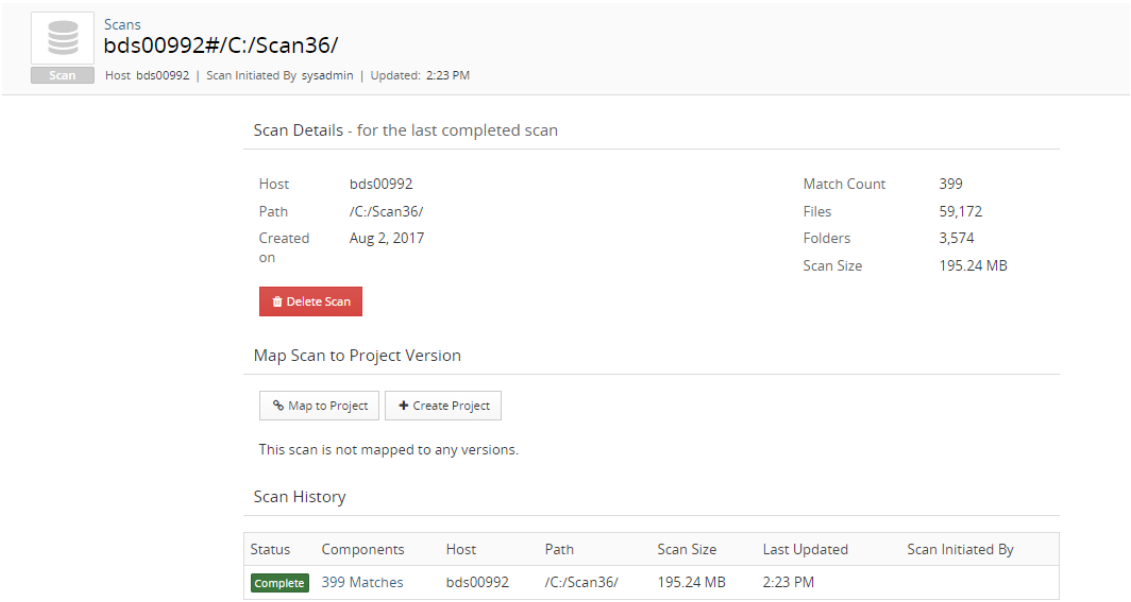
1. Log in to Black Duck and click the expanding menu ( ) icon.
2. Select **Scans**.

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



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.



   Select **Map to Project**.

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.

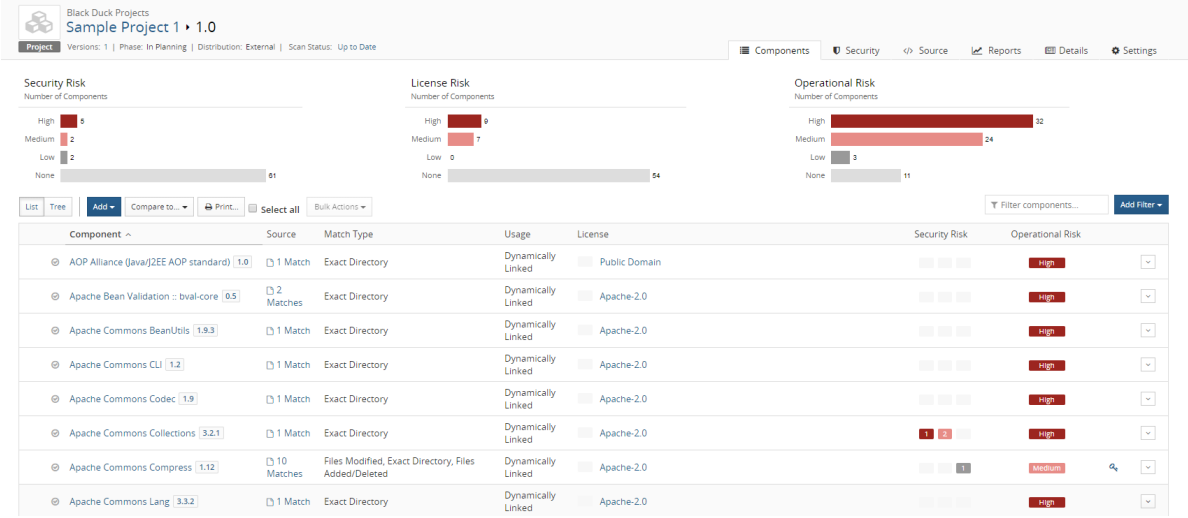
Note: Black Duck displays an aggregate project version BOM. If a component version appears more than once in an archive, it is only displayed in the BOM once.

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. Locate the internal project using the **Projects** tab on the Dashboard.
3. Select the name of the project to go to the *Project Name* page.
4. 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

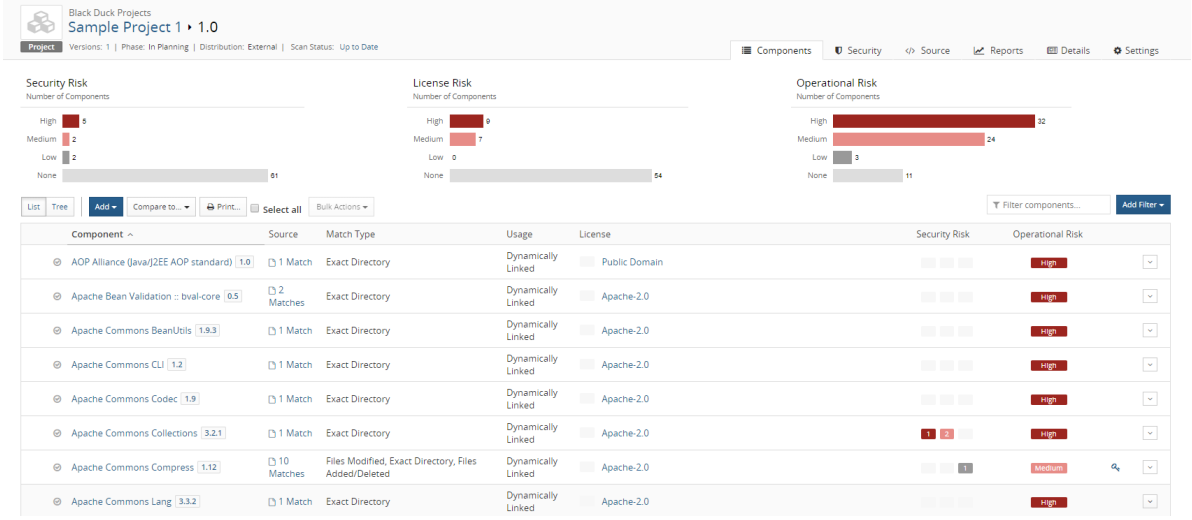
Once you have mapped a component scan to a project version, the scan results automatically create the project version's BOM. Although component scanning automatically discovers the open source component and component version from most archive files by comparing them to components in the Black Duck KB, 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.

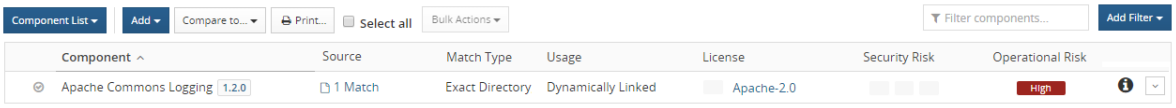
To select an alternate component and/or version match for a component in a BOM

1. Log in to Black Duck.
2. Locate the project using the **Projects** tab on the Dashboard.
3. Select the name of the project to go to the *Project Name* page.
4. Select the version name to open the **Components** tab and view the BOM.



5. In the component list view of the BOM, click and select **Edit** to open the Edit component dialog box.
6. Type the name of the OSS component in the **Component** field, and select the alternate match.
7. 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.
8. Optionally, enter a purpose for this adjustment and/or select the **Modification** checkbox and optionally, enter information regarding this modification in the field.
9. Click **Save**.

   The component and version for the BOM entry are updated. The BOM adjustment 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:

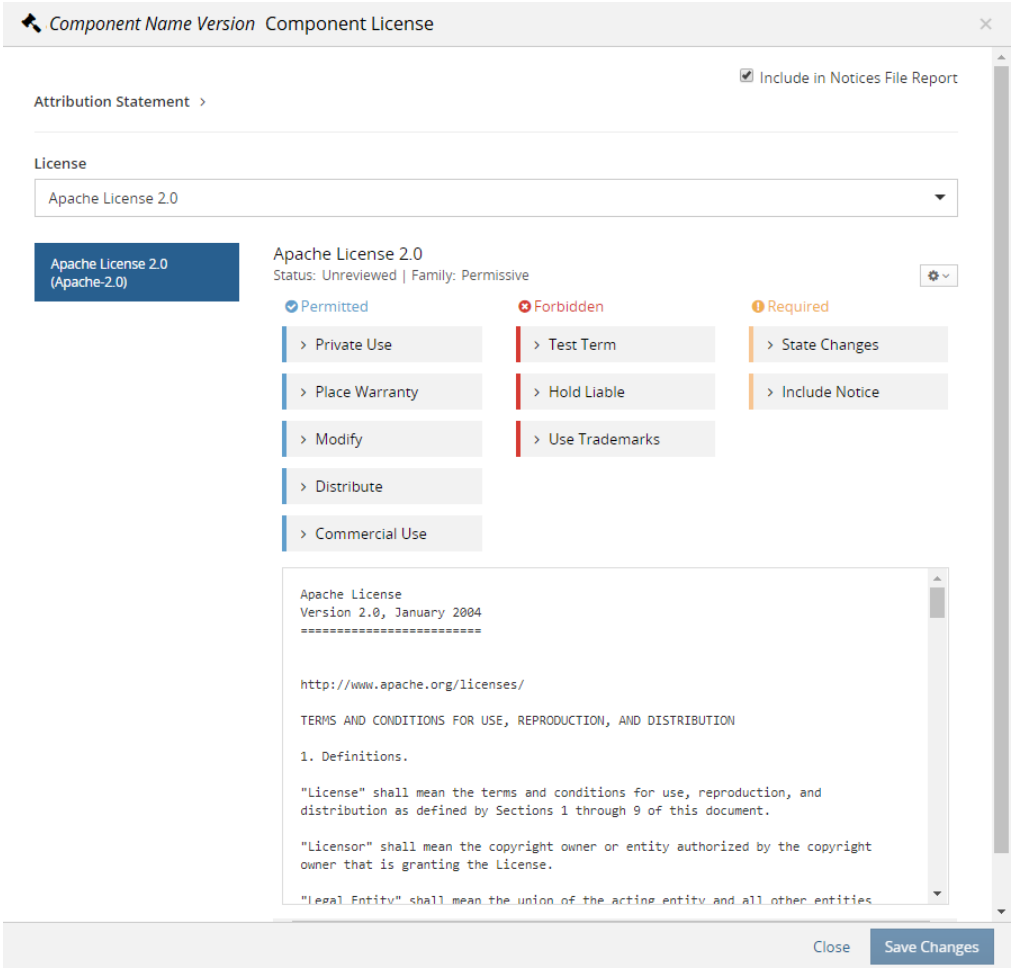


Selecting a different license for a component in a BOM

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. Locate the project using the **Projects** tab on the Dashboard.
3. Select the name of the project to go to the *Project Name* page.
4. Select the version name to open the **Components** tab and view the BOM.
5. Select the existing license to open the *Component Name Version* Component License dialog box.



Note that this version of the *Component Name Version* Component License dialog box is for those users that have the premium offering as with this module you can use this dialog box to exclude components from the Notices File report, add attribution statements, and edit license text.

6. 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.

7. 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.

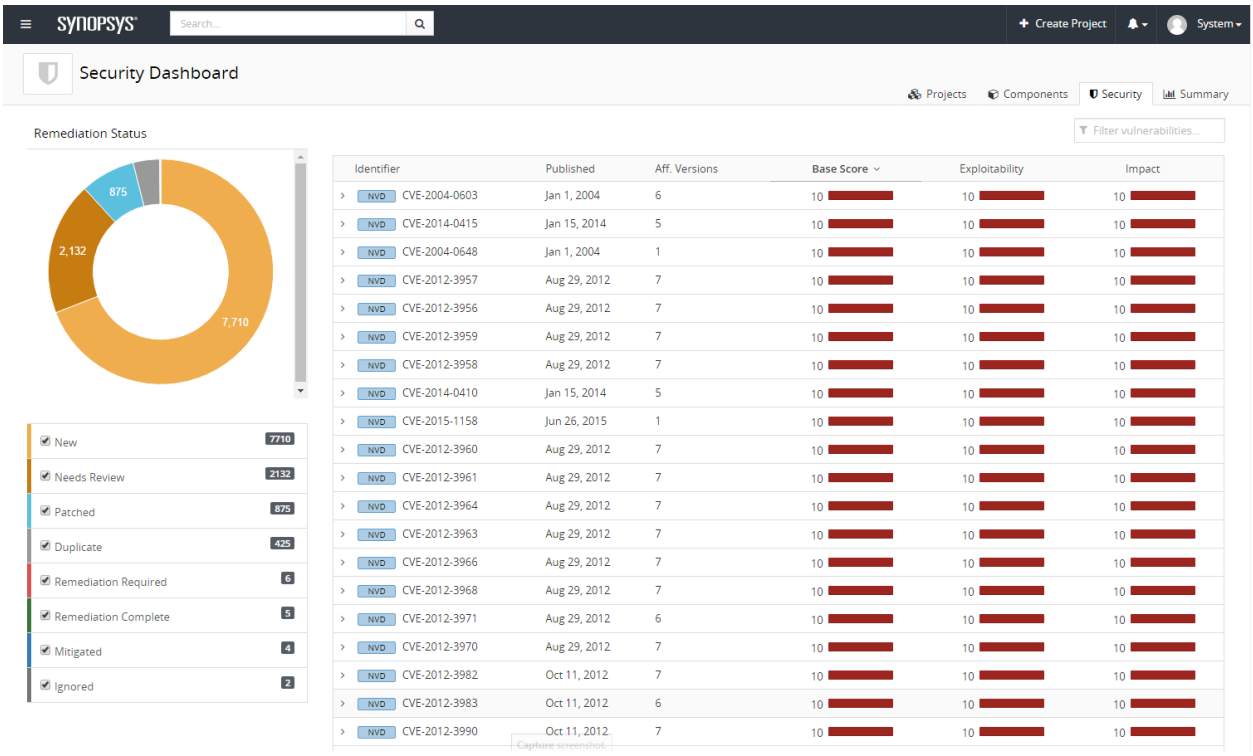
Chapter 4: About security risk

After scanning your code and mapping it to projects you can:

- Select the **Security** tab to view all the vulnerabilities that exist within your projects and their remediation status.
- Select the **Projects** tab to view the projects that have a version that has a component that has a vulnerability.
- Select the **Components** tab to view the vulnerabilities of your components.
- Select the **Summary** tab to view the overall health of the projects you have permission to view and identify areas of concern.

Viewing all security vulnerabilities

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



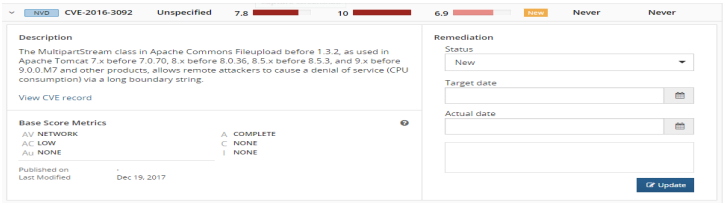
Using the Security Dashboard is an efficient way to:

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

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 table to view more information on a vulnerability by selecting **>** next to the vulnerability that interests you.



     Select to view the BDSA record, the CVE record, or the full record (VulnDB):

     a. Review the information to determine if remediation is required.

     b. If remediation is required, select one or more of the affected projects and click **Remediate**.

        You can also select in the row of a project and select **Update Remediation Plan**.

     c. Enter remediation details, such as a target date and a status, and click **Update**.

   In the **Affected Projects** tab or section, view the files related to a vulnerability by selecting in the row of a project and selecting **View related files**. The **Source** tab appears filtered to display the affected files.

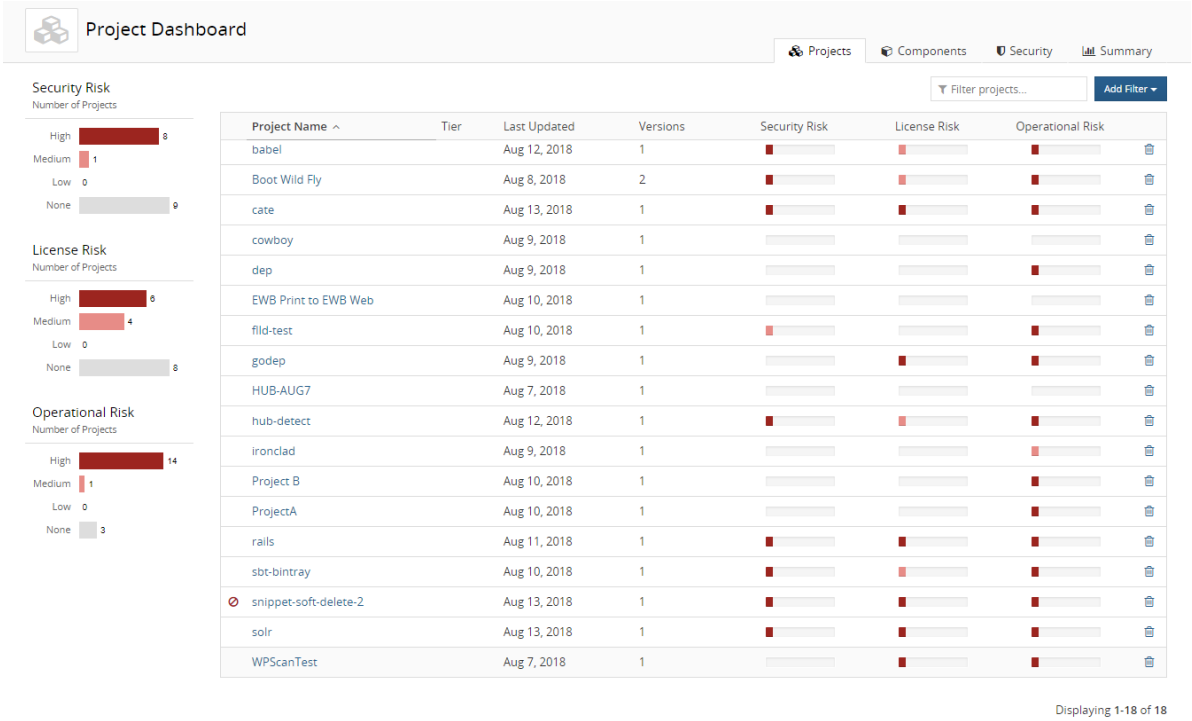
Note: A single vulnerability can be present multiple times in the remediation status pie chart since it can have multiple different remediation types within a single BOM or across multiple project version BOMs. However, a single vulnerability is listed in only one row in the table.

Viewing the security vulnerabilities of your projects and project versions

Use the Project Dashboard to view the types and severity of risk that are associated with the components that are in one or more versions of your projects. This dashboard provides an overall view of risk across all of your projects.

To view the security vulnerabilities

1. Log in to Black Duck.
2. From the Dashboard, select the **Projects** tab to display the Project Dashboard.



From this page:

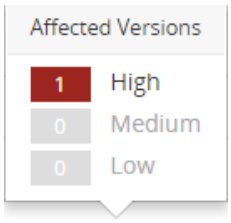
- Use the Security Risk graph to view the number of projects that have high, medium, low, or no security risk.

Select one or more values in the graph or use the filters at the top of the table to view the projects

that have one or more security risk levels.

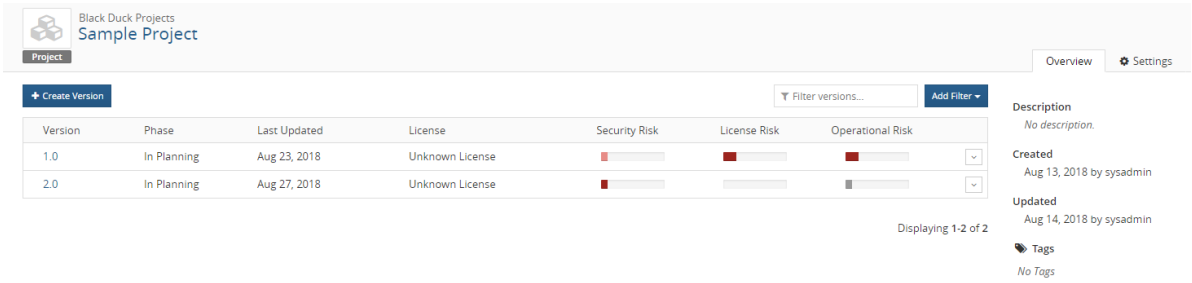
Note: The Security Risk graph displays the highest security risk level for a project, not all security levels affecting a project. Select a project name to open a page which lists all security risk levels for all versions of that project.

- Select a bar in **Security Risk** column in the table to see the number of versions of this project that are affected by a security risk.

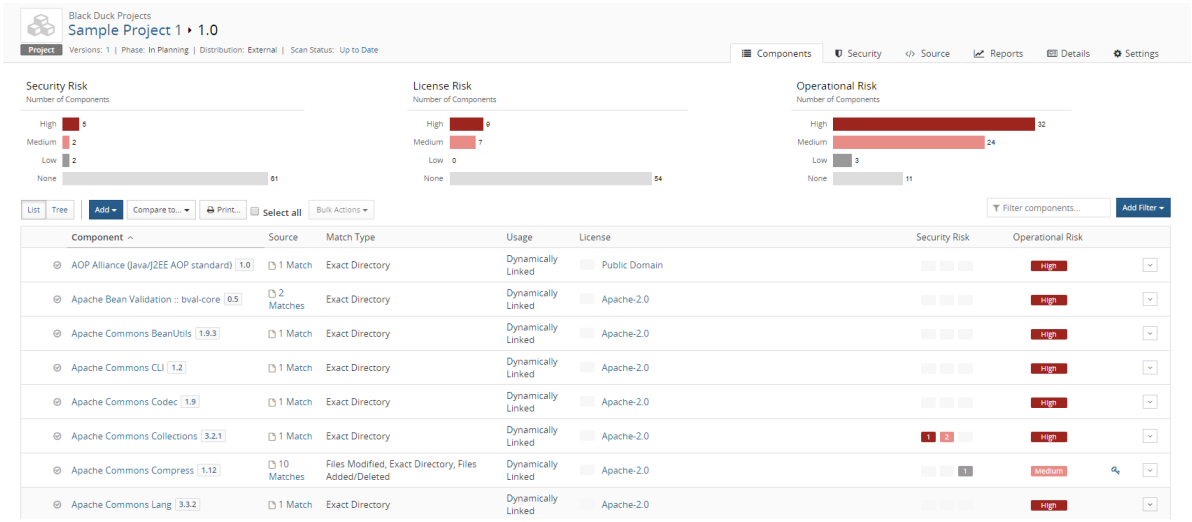


Use this column to identify the vulnerabilities that are affecting the greatest number of your projects.

3. Select a project name to view a page that lists all versions of this project.



4. Select a version with security risks to view a page which shows the BOM for this version of the project.



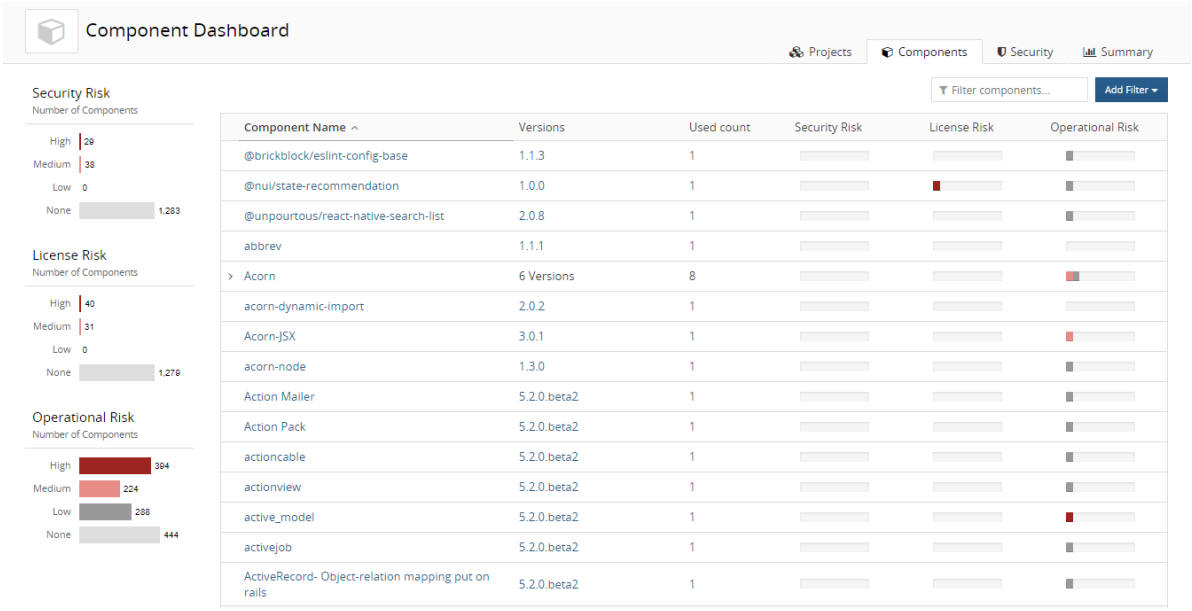
5. Use this page to view more information on the component and component version.

Viewing security vulnerabilities associated with your components

Use the Component Dashboard to view all components in your projects; components shown are top-level (parent) and subcomponents. The right side of the page displays a list of the components used in one or more of your projects. On the left side of the page risk graphs show the total number of components, used in one or more of your projects, which have each severity of security, license, and operational risks associated with them. From this page, you can drill down and view more information on these components and their vulnerabilities.

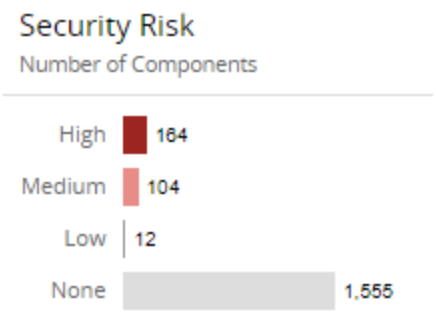
To view vulnerabilities of components in your projects

1. Log in to Black Duck.
2. Select the **Components** tab to display the Component Dashboard.



From this page:

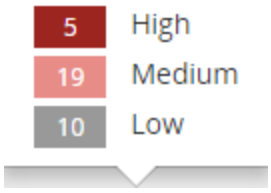
- Use the **Security Risk** graph to view the total number of components, used in one or more of your projects, that have high, medium, low, or no security risk.



Select a value in the **Security Risk** graph to view the components that have that security risk level.

Note: This graph lists the number of components which have this level of security risk as their *highest* risk level – it is not the total number of components which have this risk level. For example, if you select to view components with a medium risk level, only those components that have medium as the highest risk level appear in the table; components that have both high *and* medium vulnerabilities are not shown.

- Select a bar in **Security Risk** column in the table to identify the components that have the greatest number of vulnerabilities.

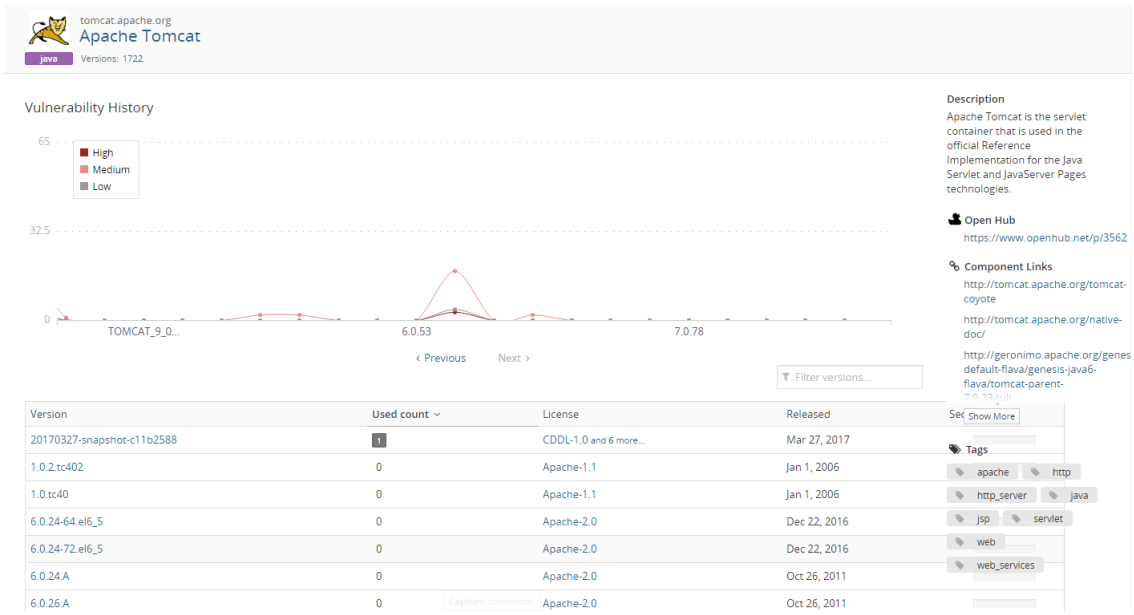


For each version of a component, the values for each risk level are calculated as:

```
# of vulnerabilities * the number of files affected by the
vulnerability for each version of the project
```

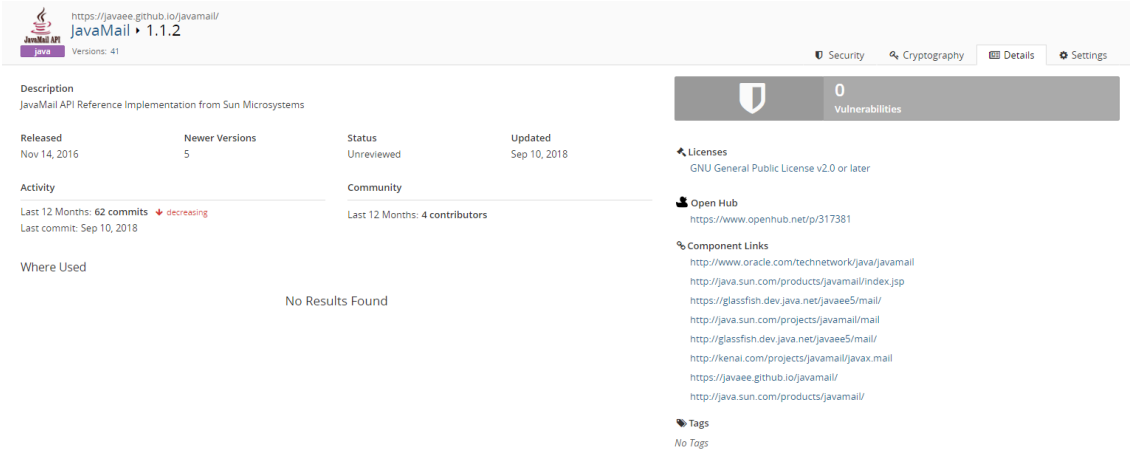
For components that have multiple versions, the total value equals the sum of all versions.

3. Click **>** for components with multiple versions to view a list of the versions used in your projects.
4. Optionally, to view the vulnerabilities for a specific version of a component:
   - Select a component name to view all versions of this component, along with a description:

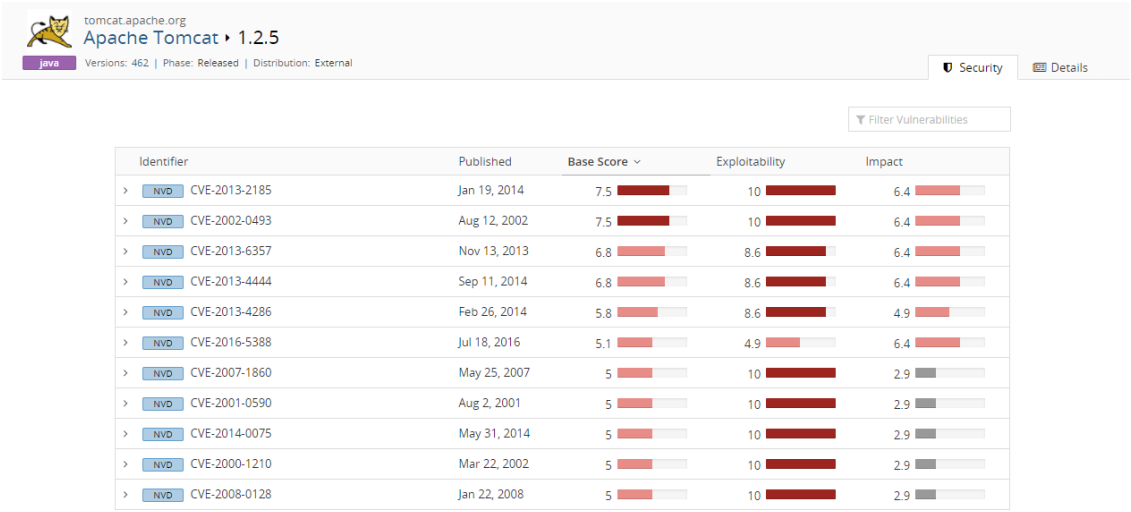


The **Used count** column shows the number of project versions that use this version of this component. A graph at the top of the page shows a history of high, medium, and low vulnerabilities for each version of this component.

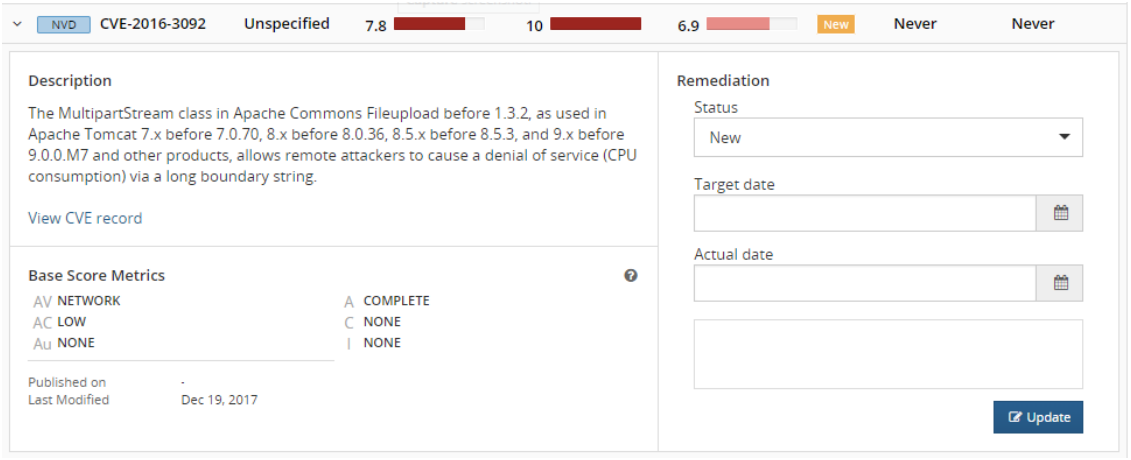
- Select a component version to view a page which lists all projects and associated versions that use this version of this component. The number of vulnerabilities, a brief description, and associated licenses with this project also appear on this page.



Click the **Security** tab to view a list of the vulnerabilities for this version of the component.



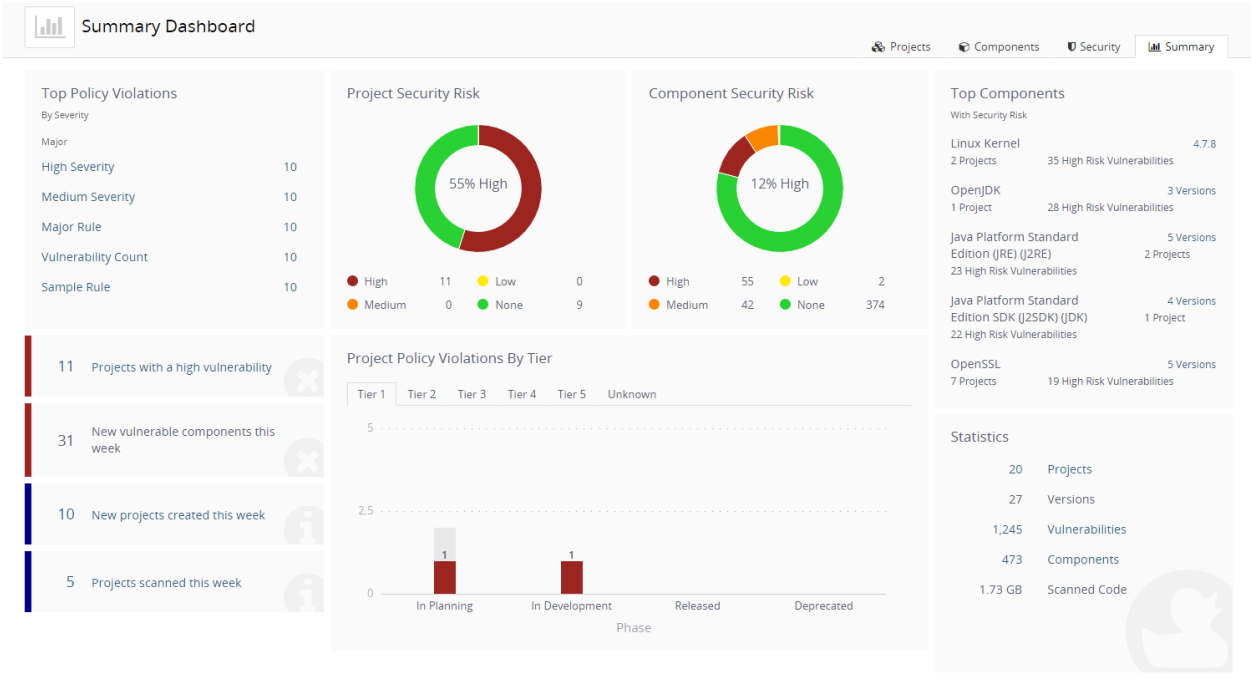
Click **>** to view more information on a vulnerability.



Select the link shown to view more information. Users with the Security Manager role who are members of the project or have project-group privileges can optionally remediate this vulnerability.

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.

Description	More Information
The **Top Policy Violations** widget displays up to the top five policy violations across all projects that you have permission to view. 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. • 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.	Select a policy rule to view the **Projects** tab filtered to display the projects with a version that violate that policy rule.
The **Project Security Risk** widget displays the number of projects you have permission to view that have a high, medium, low, or no security risk as the highest level of 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 high and medium security risks, it is counted as a project with high security risk; it is not included as a project with medium security risks.	Hover over the graph to view the number of projects with that level of security risk.
The **Component Security Risk** widget displays the number of components in projects you have permission to view that have high, medium, low, or no security risk. Note that the widget counts only the highest security risk for a component. For example, if a component has high and medium security risks, it is counted as one component with a high security risk.	Hover over the graph to view the number of components with that level of security risk.
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: • 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. Components are organized by security risk, with those components with the highest risk listed first.	Select the number of versions link to view the Component Dashboard page. Select the specific version to view the Component Version Details page.
The **Projects have a high vulnerability** widget displays the number of projects with versions that contain components with a high security risk.	Select the text to view the **Projects** tab filters to show the projects that have versions that have high security risk.
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.

Description	More Information
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.	Select the text to view the **Projects** tab which lists the projects created in the past week.
The **Projects scanned this week** widget displays the number of projects with scans from the past seven days, including today.	Select the text to view the **Projects** tab showing projects that have project versions with scans from the past week.
The **Project Policy Violations by Tier** widget displays the total number of projects by phase that have a policy violation, grouped by tiers. • 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.
The **Statistics** widget displays the following information: • **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. • **Scanned Code** lists the number of GBs scanned for all scans.	Select the projects value to view the **Projects** tab listing all projects you can view. Select the vulnerability value to view the **Security** tab filtered to show the vulnerabilities with a New, Needs Review, or Remediation Required status. Select the components value to view the **Components** tab showing all components used in the projects you can view.