BLACKDUCK | Hub

Getting Started

Version 4.4.1

This edition of the *Getting Started* refers to version 4.4.1 of the Black Duck Hub.

This document created or updated on Monday, January 15, 2018.

Please send your comments and suggestions to:

Black Duck Software, Incorporated
800 District Avenue, Suite 201
Burlington, MA 01803-5061 USA

Contents

The Hub documentation

The documentation for the Hub consists of online help and these documents:

Title	File	Description
Release Notes	release_notes_bd_hub.pdf	Contains information about the new and improved features, resolved issues, and known issues in the current and previous releases.
Installing Hub using Docker Compose	hub_install_compose.pdf	Contains information about installing and upgrading the Hub using Docker Compose.
Installing Hub using Docker Swarm	hub_install_swarm.pdf	Contains information about installing and upgrading the Hub using Docker Swarm.
Installing Hub using Kubernetes	hub_install_kubernetes.pdf	Contains information about installing and upgrading the Hub using Kubernetes.
Installing Hub using OpenShift	hub_install_openshift.pdf	Contains information about installing and upgrading the Hub using OpenShift.
Getting Started	hub_getting_started.pdf	Provides first-time users with information on using the Hub.
Scanning Best Practices	hub_scanning_best_practices.pdf	Provides best practices for scanning.
Getting Started with the Hub SDK	getting_started_hub_sdk.pdf	Contains overview information and a sample use case.
Report Database	report_db_bd_hub.pdf	Contains information on using the report database.

Hub integration documentation can be found on Confluence.

Training

Black Duck Academy 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 Black Duck Academy, 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://www.blackducksoftware.com/services/training

View the full catalog of courses and try some free courses at https://academy.blackducksoftware.com

When you are ready to learn, log in or sign up for an account: https://academy.blackducksoftware.com

Customer Success Community

The Black Duck Customer Success Community is our primary online resource for customer support, solutions and information. The Customer Success 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 Customer Success 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, please send an email to communityfeedback@blackducksoftware.com or call us at +1 781.891.5100 ext. 5.

To see all the ways you can interact with Black Duck Support, visit: https://www.blackducksoftware.com/support/contact-support.

Chapter 1: Logging in to the Hub

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

Using the Hub, 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 the Black Duck Hub lets you search projects that may be restricted to team members or company employees.

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

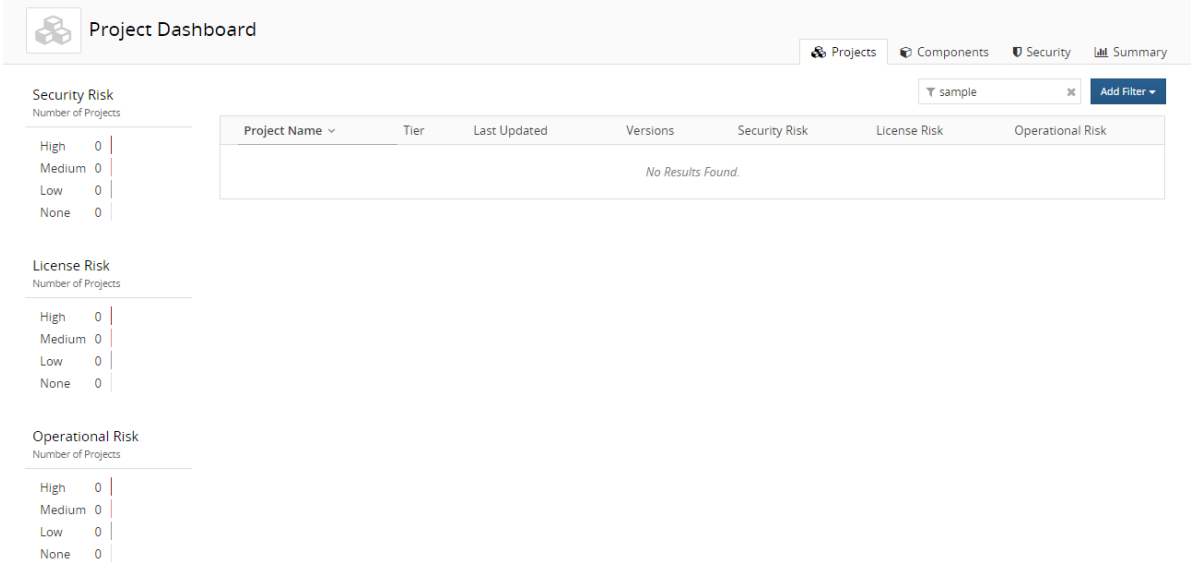
To log in to the Hub

1. Using a browser, navigate to the Hub 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 Hub administrator.

   Note: Your password is case sensitive.

3. Click **Login**.

   When you log in, the Hub displays your Dashboard page.



When you first log in after installing the Hub, an empty Dashboard page appears. For information to appear in the Hub, 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 Hub: Using the Hub Scanner course on Black Duck Academy. You will learn how to use both the Hub 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.

Hub Scanner client requirements

A Windows 7 or later, Mac OS X 10.9 or later, or Linux 64-bit system is required to run the Hub Scanner. Client systems must have a minimum of 6 GB of RAM.

Running a component scan using the Hub Scanner 2.0

The Hub Scanner 2.0 provides a new interface (GUI) to make it easier to scan code.

With the Hub Scanner, you can:

- Create a scan file to be uploaded at a later time.
- Scan files and immediately upload the scan file to the Hub.
- View scans in the Hub.
- Manage scan files.
- Upload scan files directly to the Hub.

To use the Hub Scanner GUI:

1. Download and install the Hub Scanner.
2. Configure the Hub Scanner with your Hub server settings and complete the installation process.
3. Use the Hub Scanner to scan and/or upload your files.

Note: An error message appears if you exceed the scan size limit, which is typically 5 GB. Contact Customer Support if you receive this message.

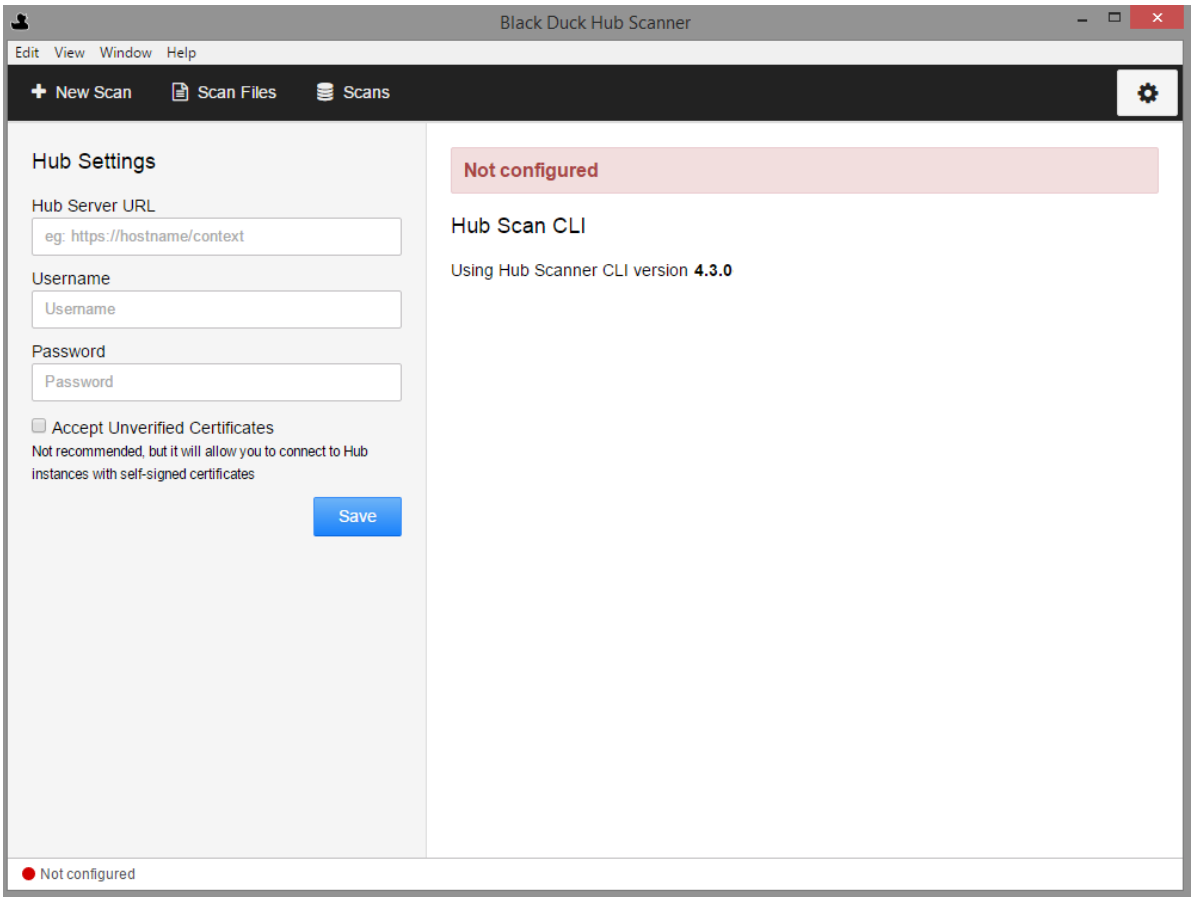
Downloading and installing the Hub Scanner

1. Log in to the Hub.
2. Select  and select **Tools**.
3. Select the operating system you wish to use in the **Hub Scanner** section and select the **Desktop** link to download the Hub Scanner 2.0.
4. Run the executable to install the Hub Scanner GUI.

Configuring the Hub Scanner

After installing the Hub Scanner GUI, continue the installation process by configuring your Hub settings and downloading the Hub Scanner client.

1. Click  in the Hub Scanner.



2. Enter the following information:
   - The Hub Server URL. Enter the URL to the Hub 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.

- The Black Duck Hub user account with the code scanner role.
- The password of the user account with the code scanner role.

3. Select **Accept Unverified Certificates** if you are trying to connect to a Hub instance that uses a self-signed or invalid certificate. By default, the Hub Scanner will not allow connections to that server.
4. Click **Save**. The Hub Scanner connects to the Hub server and displays the version of the Hub you are connected to and the Hub Scan CLI.
5. Click **Download Hub CLI *Version Number***.

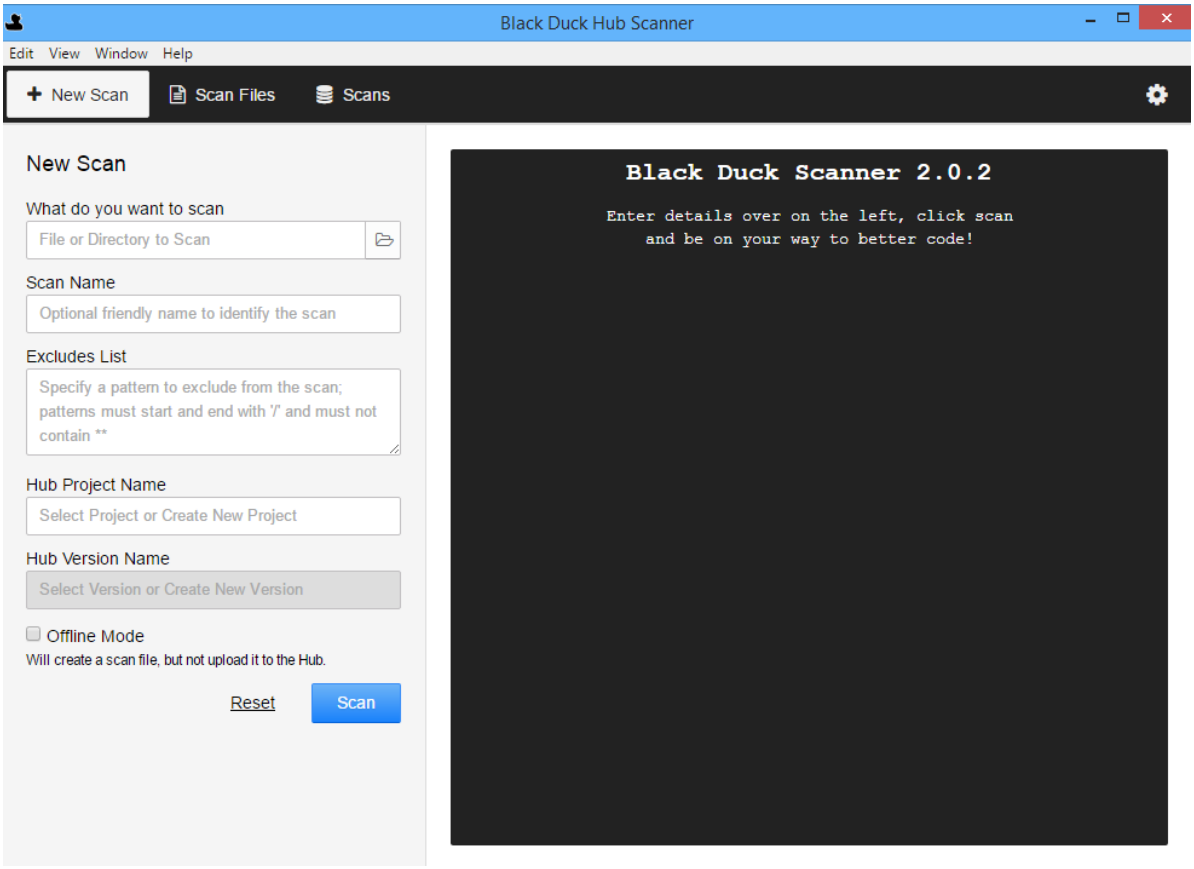
   The Hub Scanner client is downloaded and installed.

Creating a scan file

You can use the Hub Scanner to output the scan to a file which you can later upload to the Hub by using the Hub Scanner, either by using the GUI, (as described below), the command line, or by using the Hub UI.

To create a scan file:

1. Click **New Scan**.

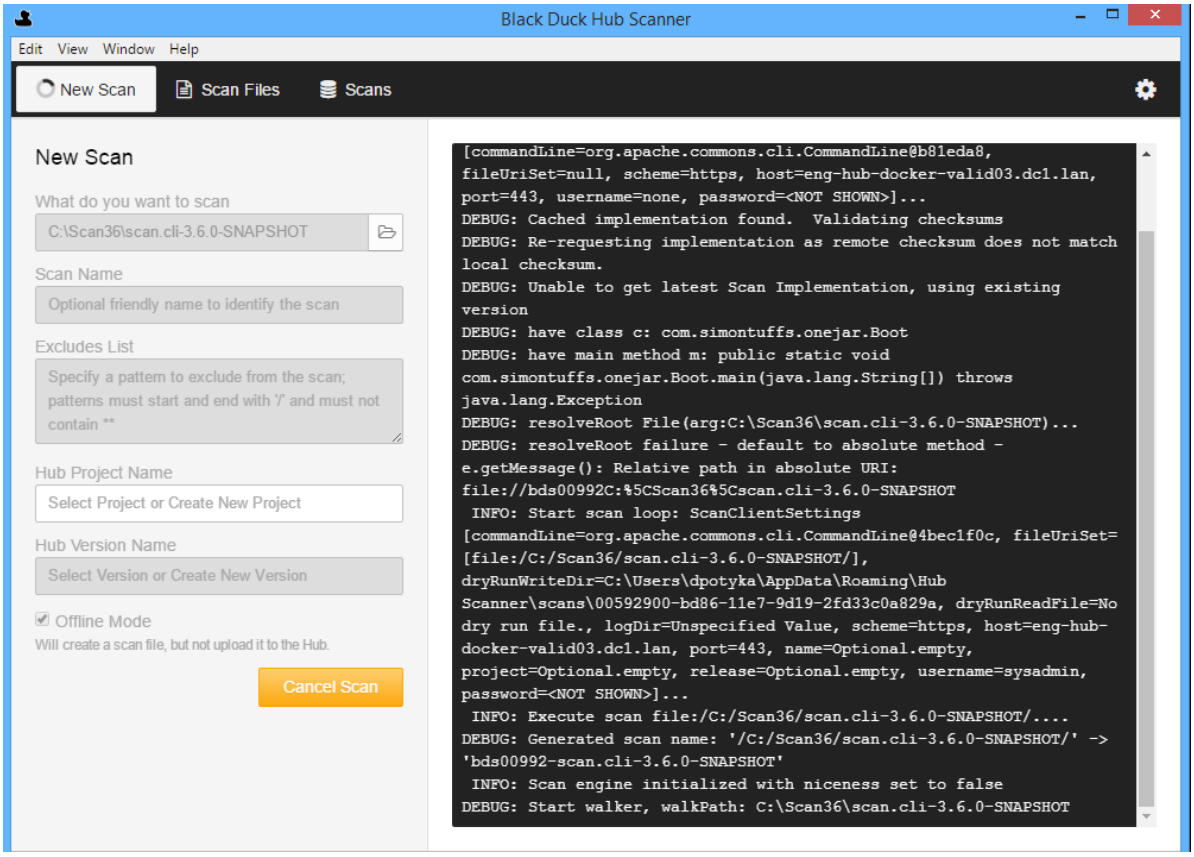


2. In the **What do you want to scan** field, enter the file or directory to scan or click to open a dialog box to select the directory or file to scan.

3. Optionally, enter the following:
   - **Scan Name**. The name of the scan.
   - **Excludes List**. Specify a list of directories to exclude from the scan. Directories should be separated by commas or new lines and have leading and trailing forward slashes (/). For more information, refer to the Hub online help.
   - **Hub Project Name**. The name of the project to which you want to map the scan results.
     - If the project exists, the Hub Scanner maps the scan results to the project.
     - If the project does not exist, the Hub Scanner creates the project.
   - **Hub Version Name**. The version of the project to which you want to map the scan results.
     - If the project and project version exist, the Hub Scanner maps or remaps the scan results.
     - If the project exists, but the version does not, the Hub Scanner creates the version and maps the scan results.

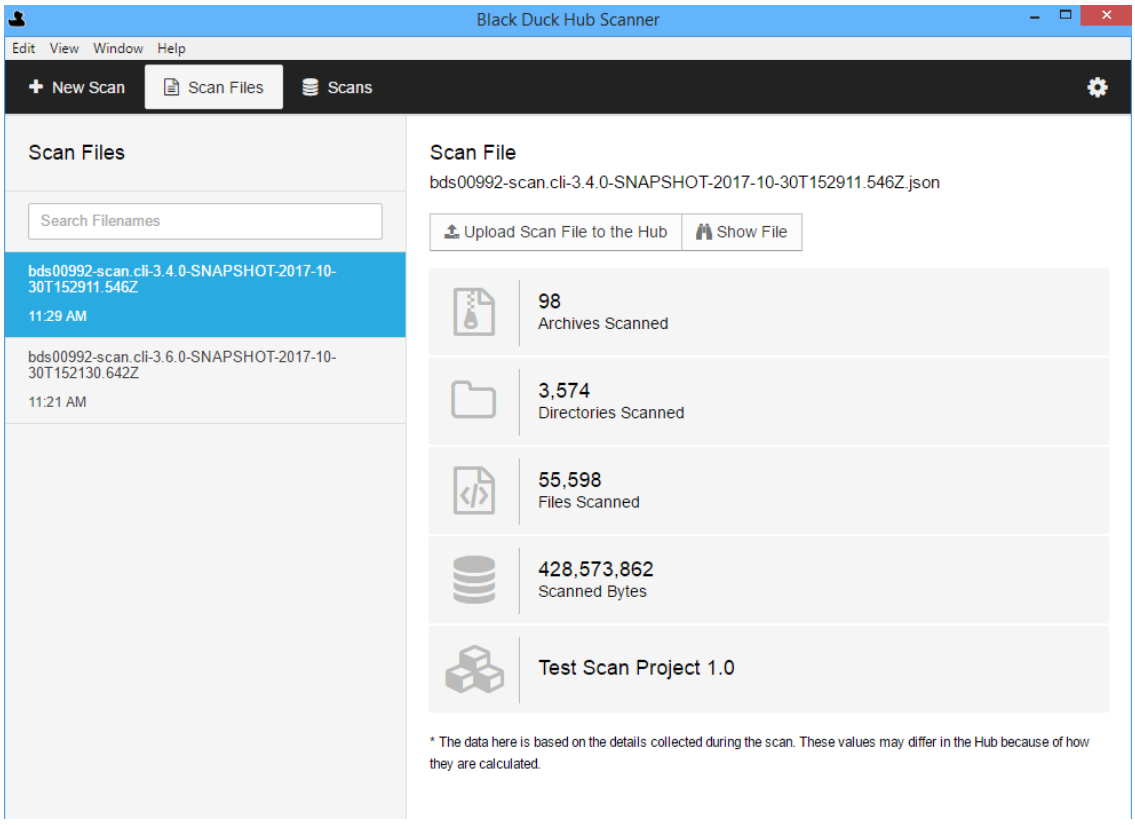
4. Select **Offline Mode**.
5. Click **Scan**.

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



When the scan is complete, select the **Scan Files** tab to view information on the completed scan. From this tab, you can:

- View scan information by selecting the scan name in the left column. Scan information appears in the right column:



Use this tab to manage your scan, as described in the next section.

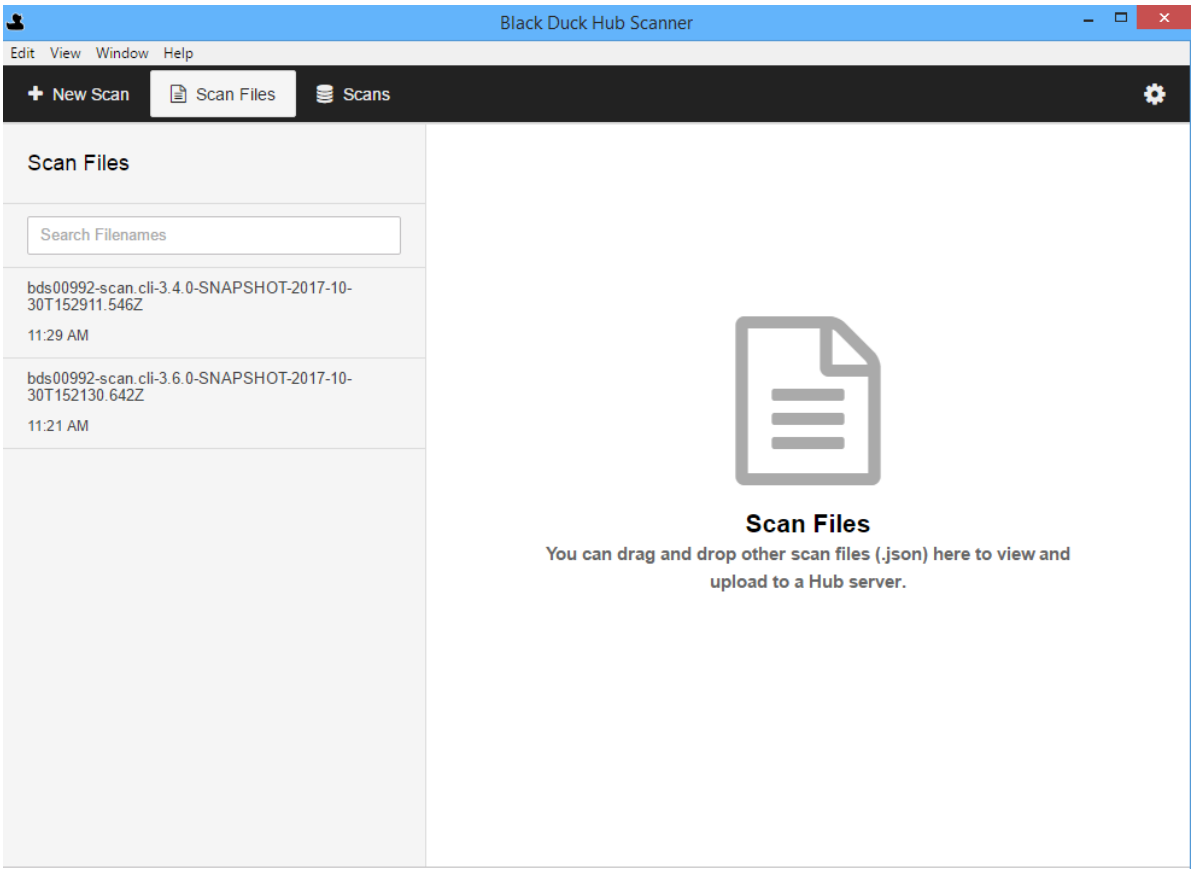
Managing scans

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

1. Click **Scan Files**.

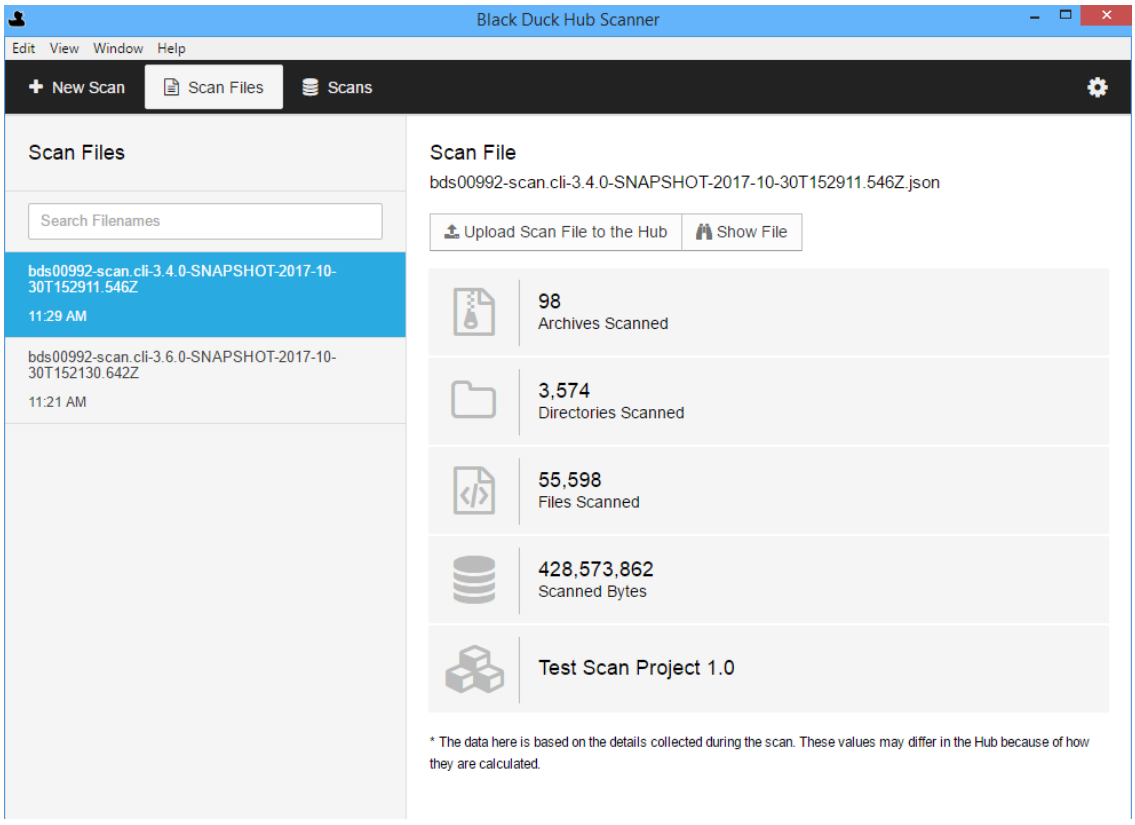
   A list of scans appear in the left column of the tab.

   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:



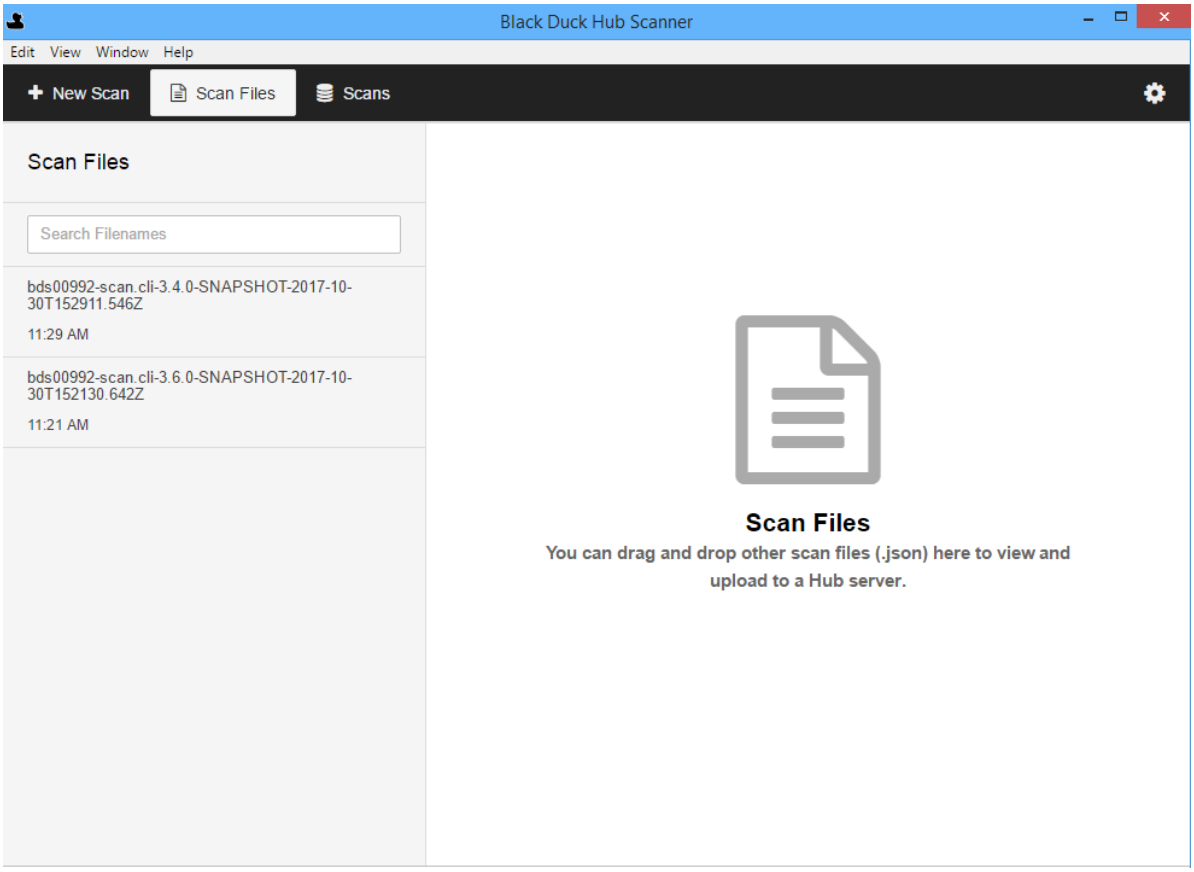
- View the location of the file on your system by clicking **Show File**.
- Upload the file, as described in the next section.
- Delete the scan by hovering over the scan name in the left column and clicking **Delete**. Click **Yes** to confirm.

Uploading scan files to the Hub

You can use the Hub Scanner to upload scan files to the Hub.

Drag and drop scan files on your local machine to the **Scan Files** tab.

1. Click **Scan Files**.



2. Select the file to upload.
3. Click **Upload Scan File to the Hub**. The Upload Progress window appears showing you the status of the upload. Close the window when the process is complete.

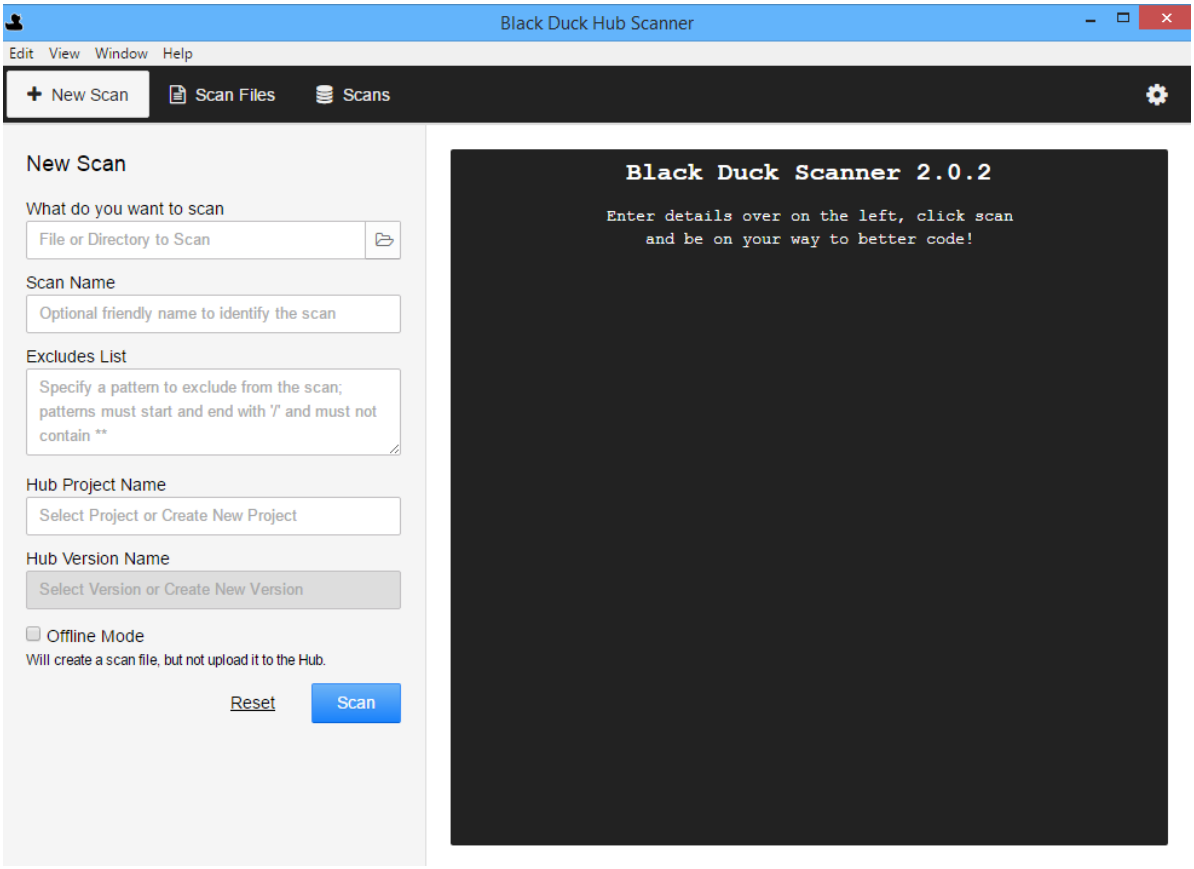
   You can confirm that the scan has been uploaded by clicking **Scans** and viewing the uploaded file.

Scanning directly to the Hub

Use this procedure to scan and upload the scan file directly to the Hub.

If you enter a project name and version, the scan is also automatically mapped. If you do not select a project name or version name, the file is uploaded but not mapped.

1. Click **Scan**.



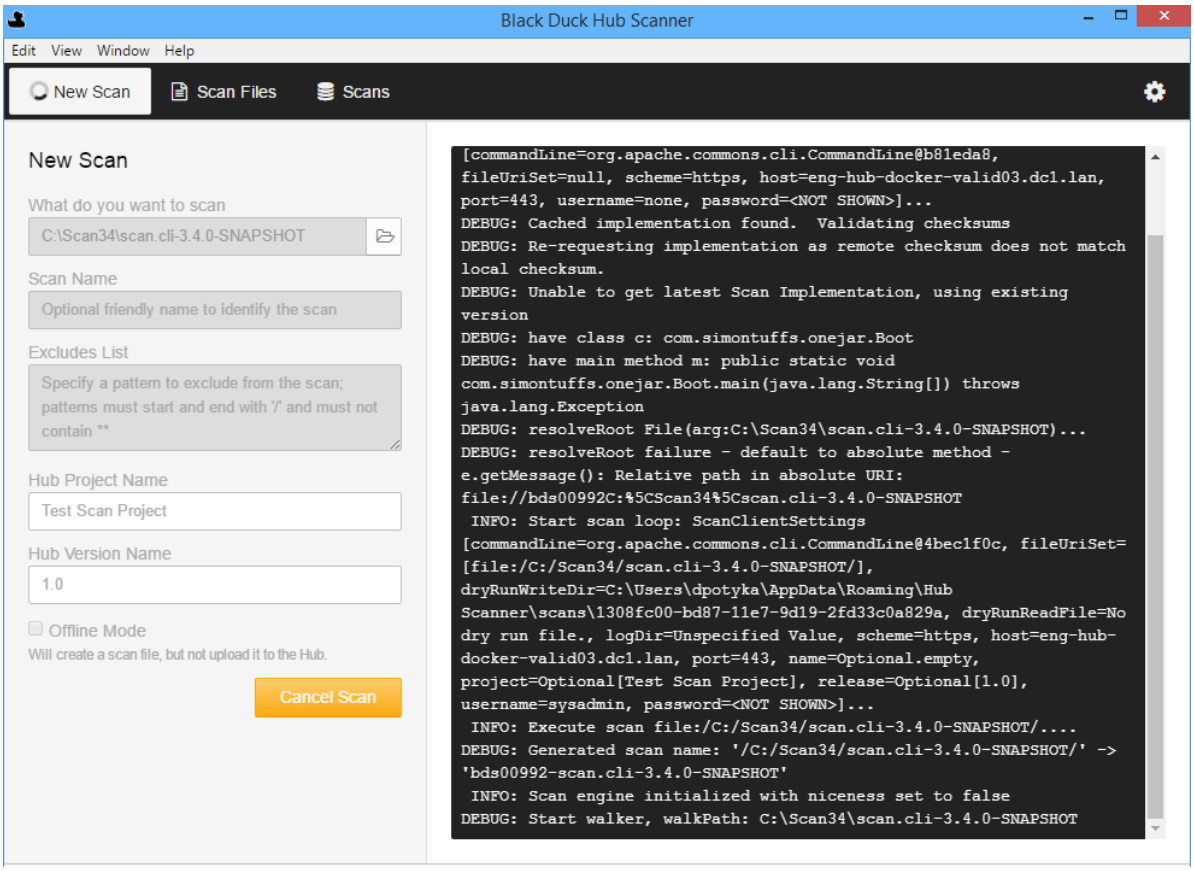
2. In the **What do you want to scan** field, enter the file or directory to scan or click to open a dialog box to select the directory or file to scan.

3. Optionally, enter the following:
   - **Scan Name**. The name of the scan.
   - **Excludes List**. Specify a pattern to exclude from the scan. Use the command line to specify a directory or directories you want to exclude from scanning. For more information, refer to the Hub online help.
   - **Hub Project Name**. The name of the project to which you want to map the scan results.
     - If the project exists, the Hub Scanner maps the scan results to the project.
     - If the project does not exist, the Hub Scanner creates the project.
   - **Hub Version Name**. The version of the project to which you want to map the scan results.
     - If the project and project version exist, the Hub Scanner maps or remaps the scan results.
     - If the project exists, but the version does not, the Hub Scanner creates the version and maps the scan results.

4. Clear the **Offline Mode** option.

5. Click **Scan**.

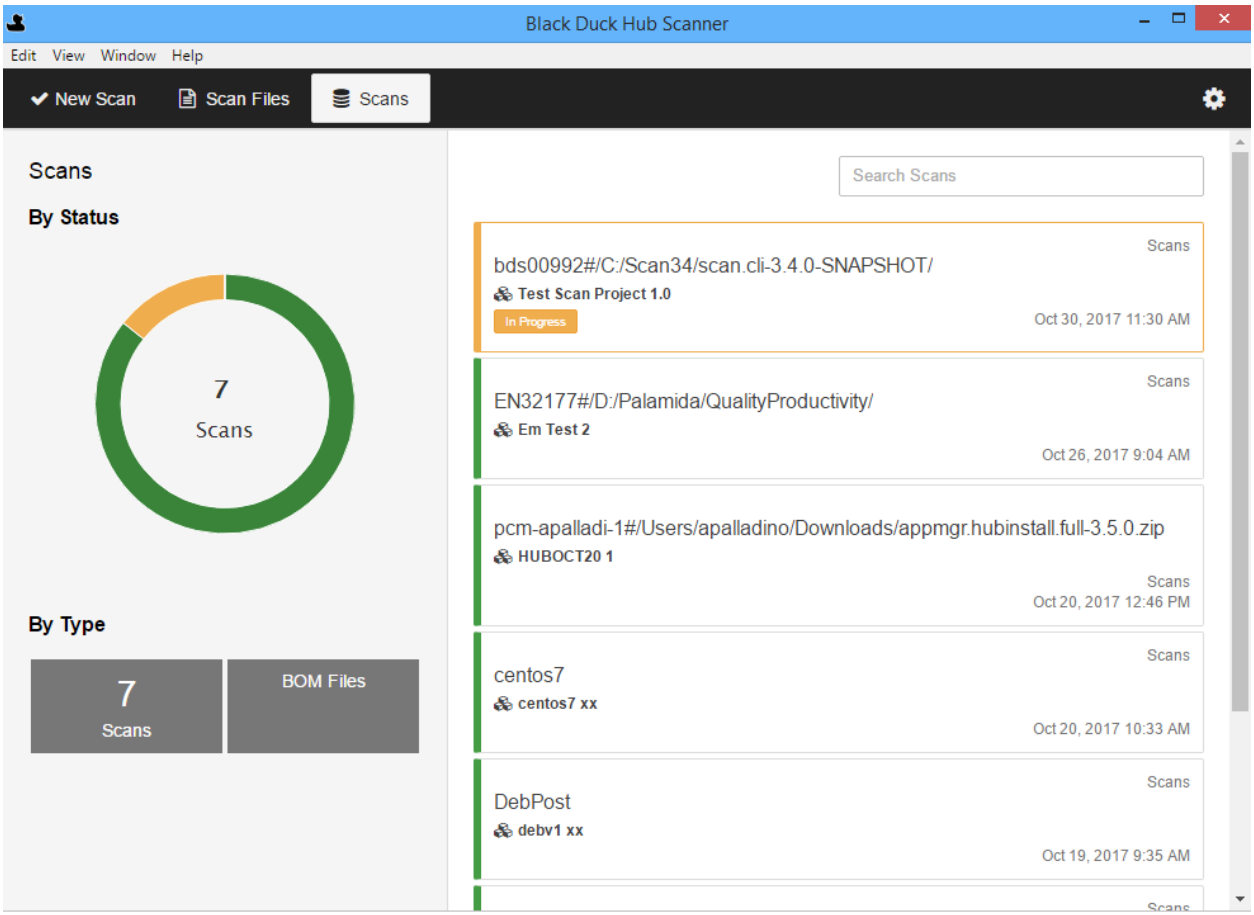
   The status of the scan appears on the right side of the window. An option to cancel the scan appears.



   You can view the uploaded scan using the **Scans** tab as described in the next section.

Viewing Scans

You can view the scans that have been uploaded to the Hub UI by clicking **Scans**:



This tab displays the following information:

- The left side of the tab shows uploaded scans by status and by type (Scans and BOM files).
- 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.
  - Type (Scan or BOM file)
  - Date and time scan was uploaded to the Hub.

  Note that information will not appear for BOM files.

Use the filter to limit the scans shown.

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

Creating a project

A project is the base unit in the Hub. 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. All users can create a project in the Hub.

Only users with the Code Scanner or Sysadmin role can create projects.

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

Tip: Want to Learn More? Check out the Black Duck Hub: Creating Projects course on Black Duck Academy. You wi'll learn how to create and save a Black Duck Hub project as well as how to change overall project settings.

To create a project

1. Log in to the Hub.
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 the Hub, 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, the Hub adds the user to the project team.

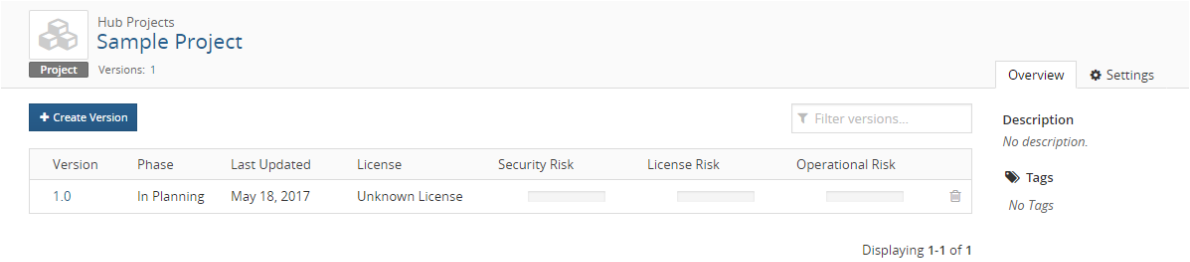
   - Select a tier. [1]
5. Type the version for this project in the **Version** field.
6. Optionally, select **Add version details** to enter additional information such as the planned release date, the project phase, and the method in which the project is being delivered.
7. By default, edits to a version of this project apply to all versions of this project, excluding archived

[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.

versions and manually added components. Clear this option if you want edits to apply to specific versions only.

8. Click **Create**.

   The Hub displays the *Project Name* page.



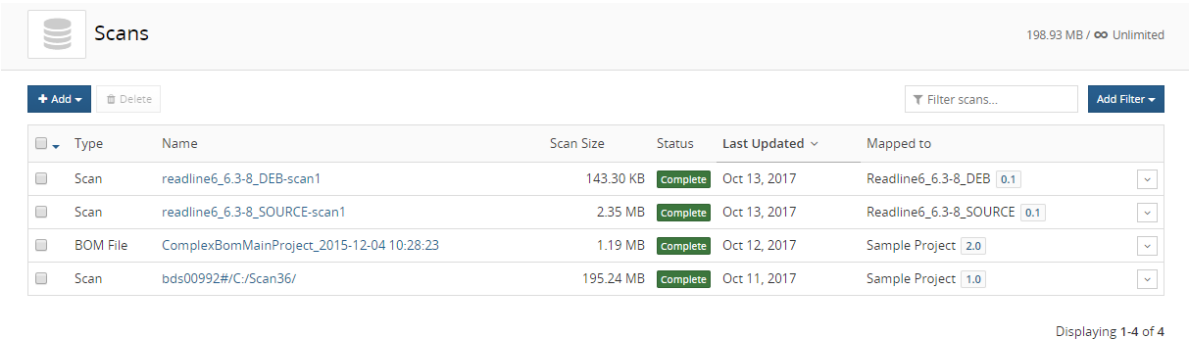
Mapping a scan to a project

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, the Hub automatically updates the BOM of the project with any new information discovered during subsequent scans.

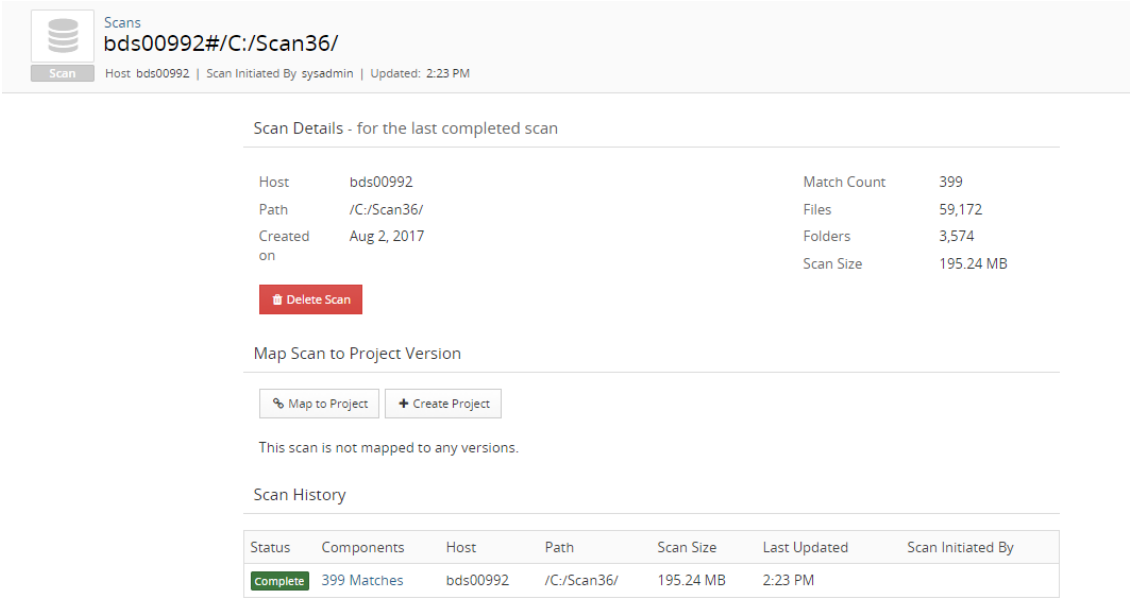
To map a scan to a project

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



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**.

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

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

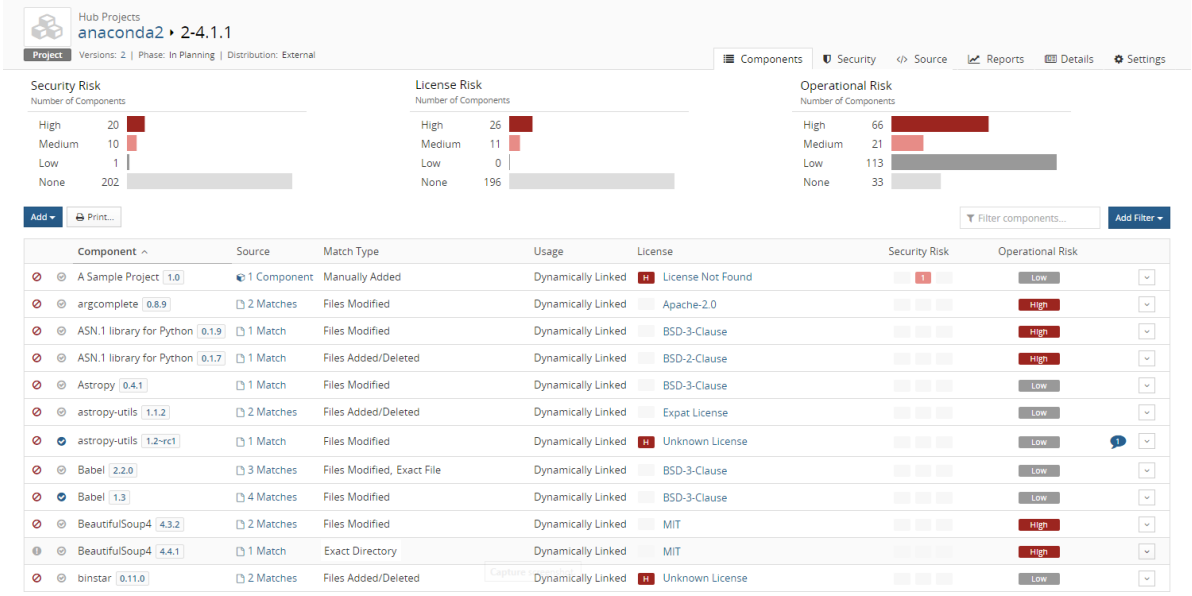
Chapter 3: Viewing your BOM

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 the Hub.
2. Locate the internal project using the **Projects** tab on the Dashboard.
3. Select the name of the internal project to go to the Hub Internal Projects page.
4. Select the version name of the project that you want to view.

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



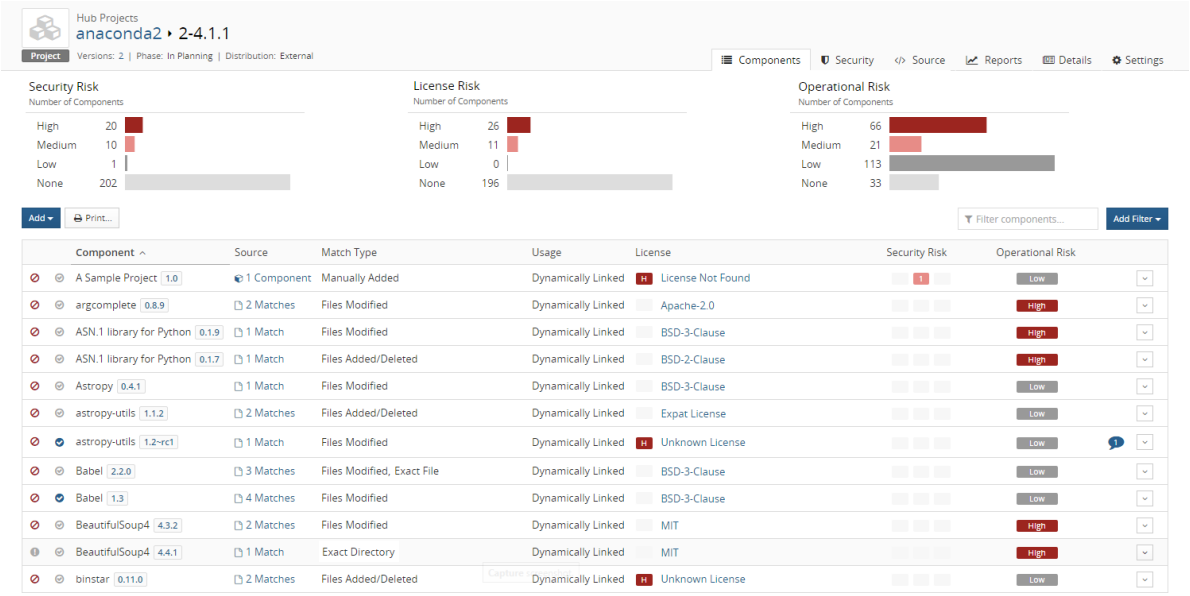
Adjusting the component and/or component version in a project version BOM

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 OSS component that is not available in the Black Duck KB, or you may be using a modified version of an OSS component. You can adjust the component and version for an OSS component in a BOM.

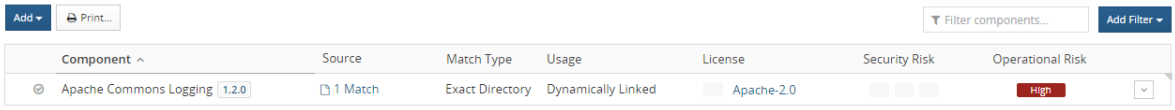
To select an alternate component and/or version match for an OSS component in a BOM

1. Log in to the Hub with the BOM Manager role.
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. 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 OSS component from the **Version** list. The list contains all versions of the OSS component that are available in the Black Duck KB.
8. Click **Save**.

   The component and version for the BOM entry are updated. The BOM adjustment indicator appears in right corner of table row to indicate that the component and/or version were changed from the one automatically discovered in the component scan:

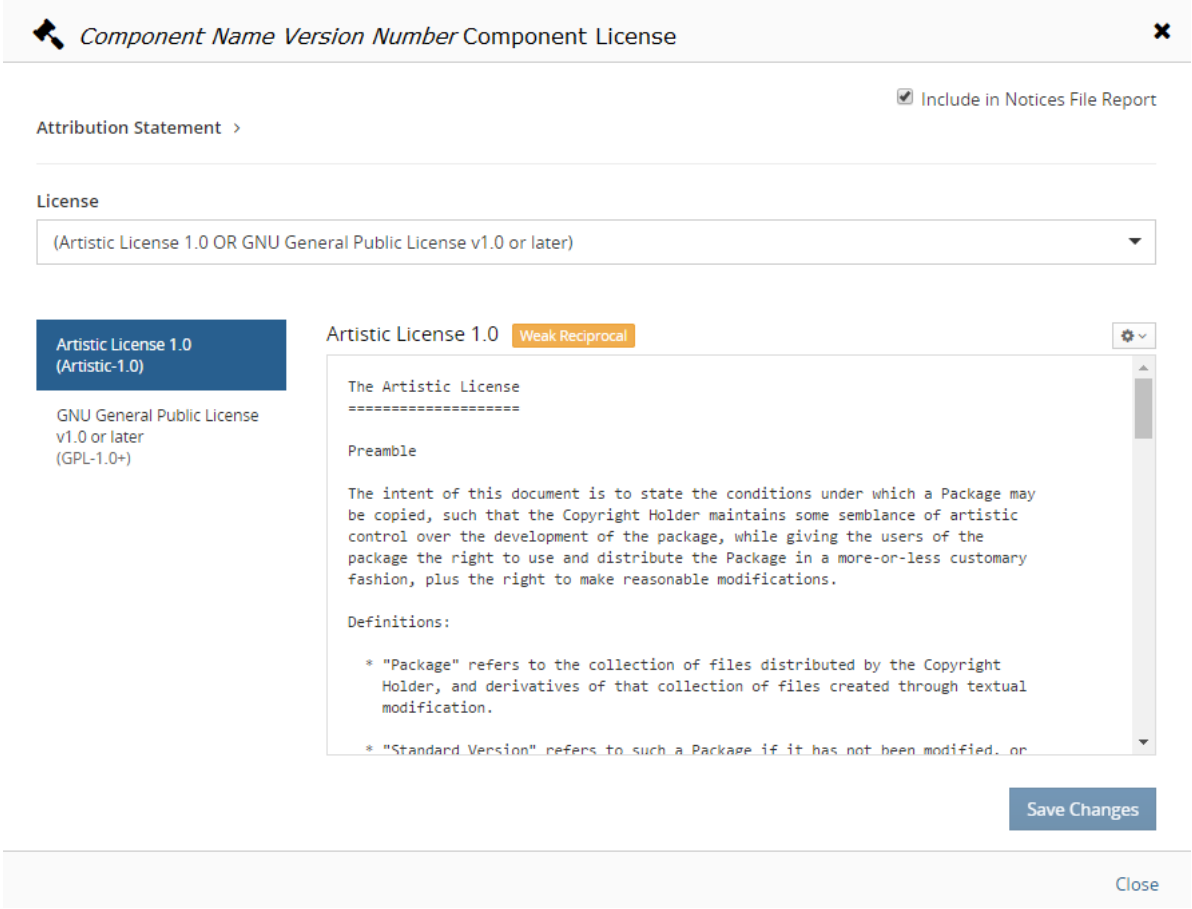


Selecting a different license for an OSS component in the project version BOM

You can select a license for an component used in a BOM that is different from the OSS 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 the Hub with the BOM Manager role.
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 OSS component and for the project version are updated.

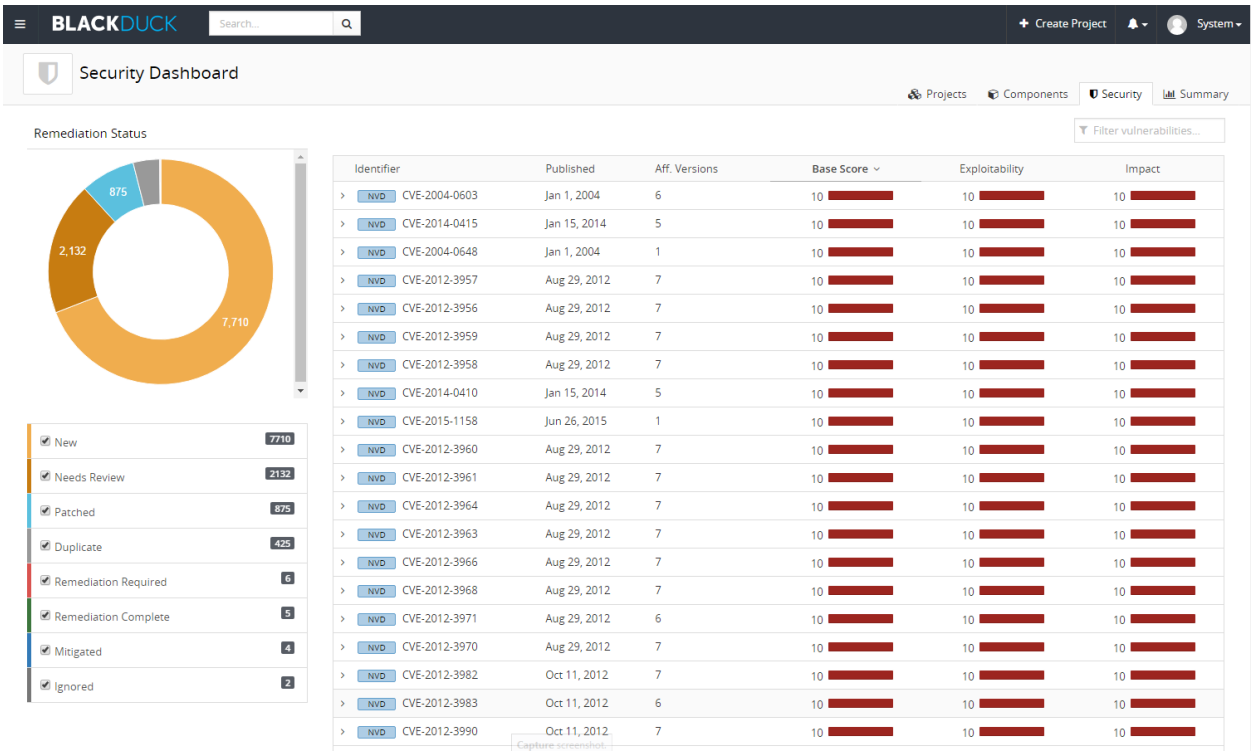
Chapter 4: About security risk

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.



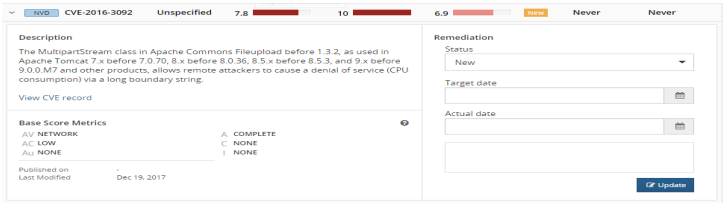
Using the Security Dashboard is an efficient way to:

- 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 the Hub.
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**.

      Note: Only users with the BOM Manager role can remediate an affected project.

      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.

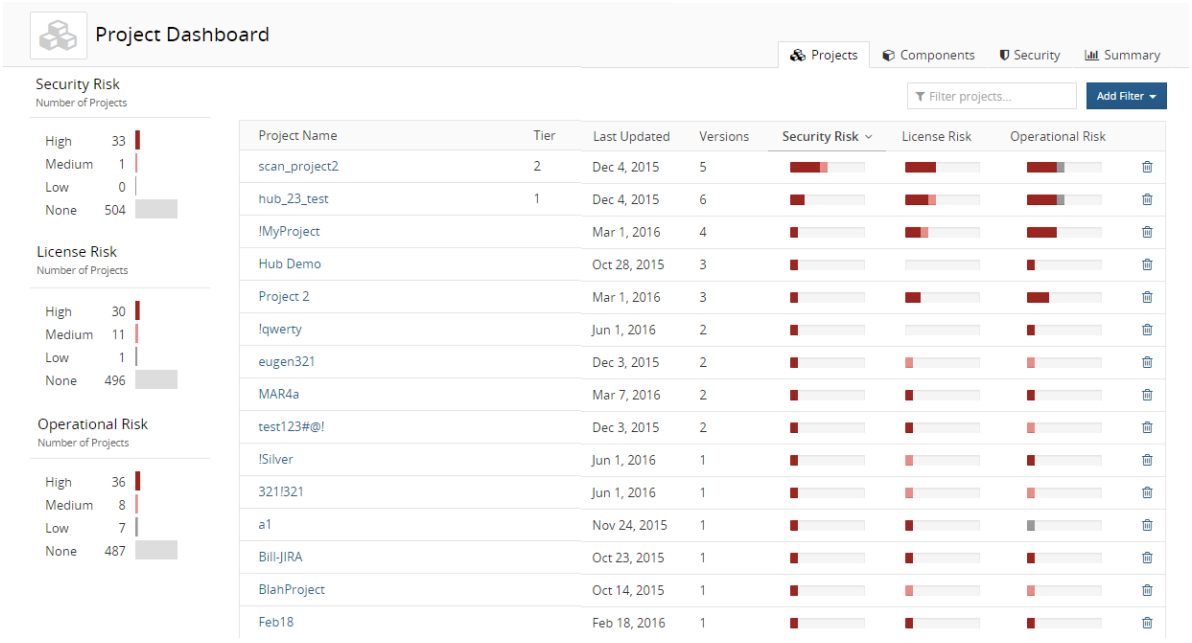
Note: A single vulnerability can be present multiple times in the remediation status pie chart since it can have multiple different remediation types within a single BOM or across multiple project version BOMs. However, a single vulnerability is listed in only one row in the table.

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 the Hub.
2. From the Dashboard, select the **Projects** tab to display the Project Dashboard.



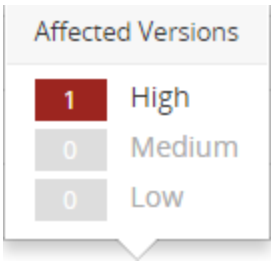
From this page:

- 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.

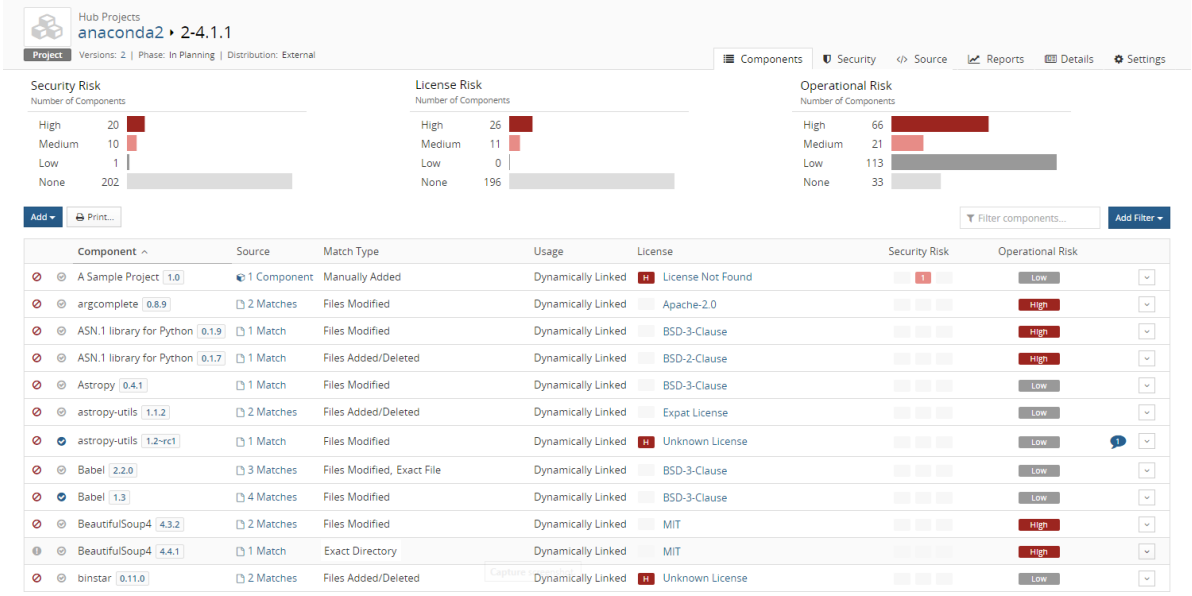
- Select a bar in **Security Risk** column in the table to see the number of versions of this project that are affected by a security risk.



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.



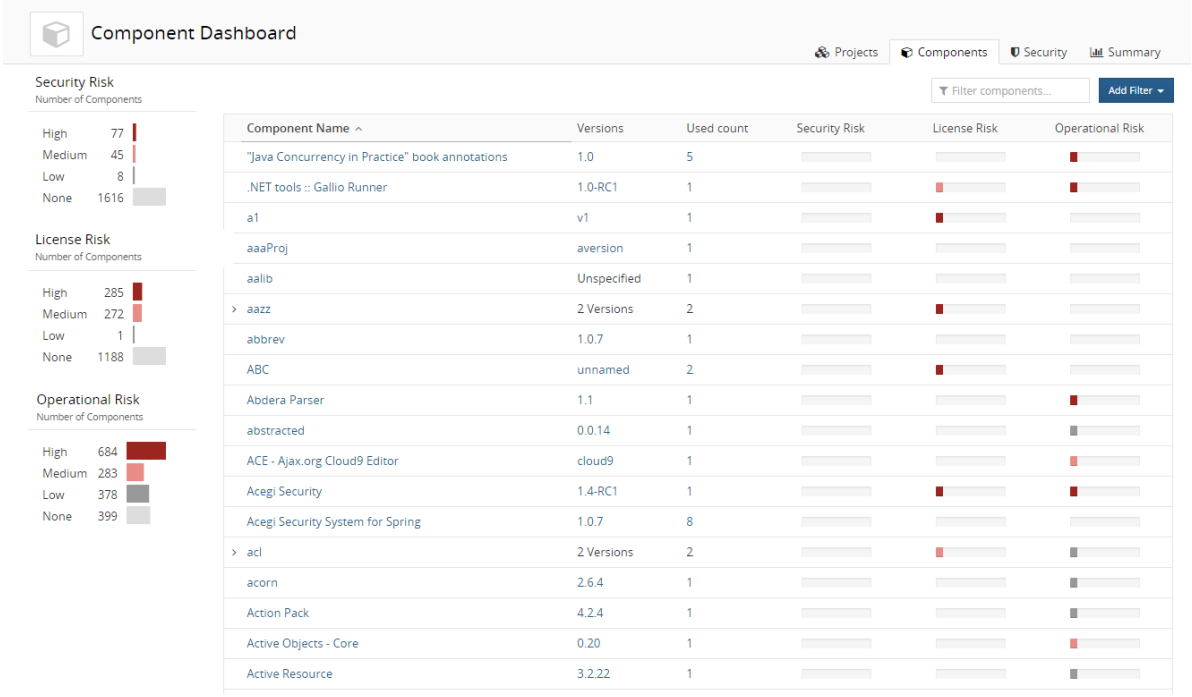
5. Use this page to view more information on the component and component version. Users with the BOM Manager role can ignore the component.

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.

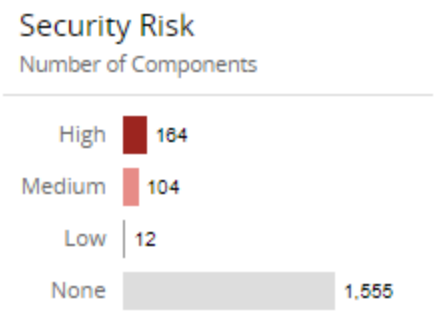
To view vulnerabilities of components in your projects

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



From this page:

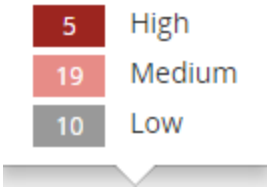
- Use the **Security Risk** graph to view the total number of components, used in one or more of your projects, that have high, medium, low, or no security risk.



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.

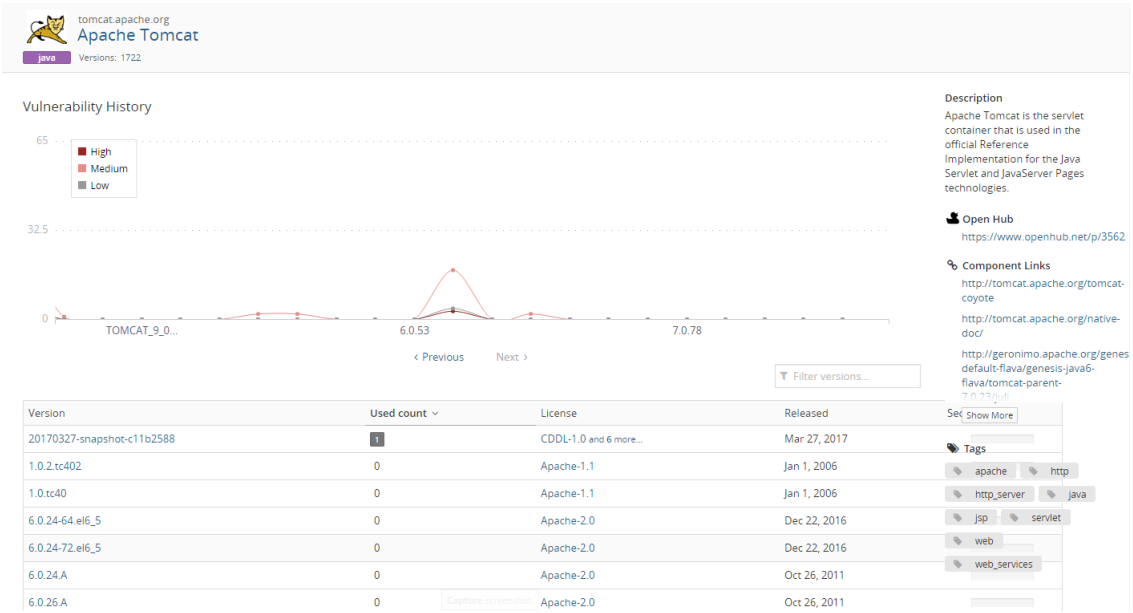


For each version of a component, the values for each risk level are calculated as:

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

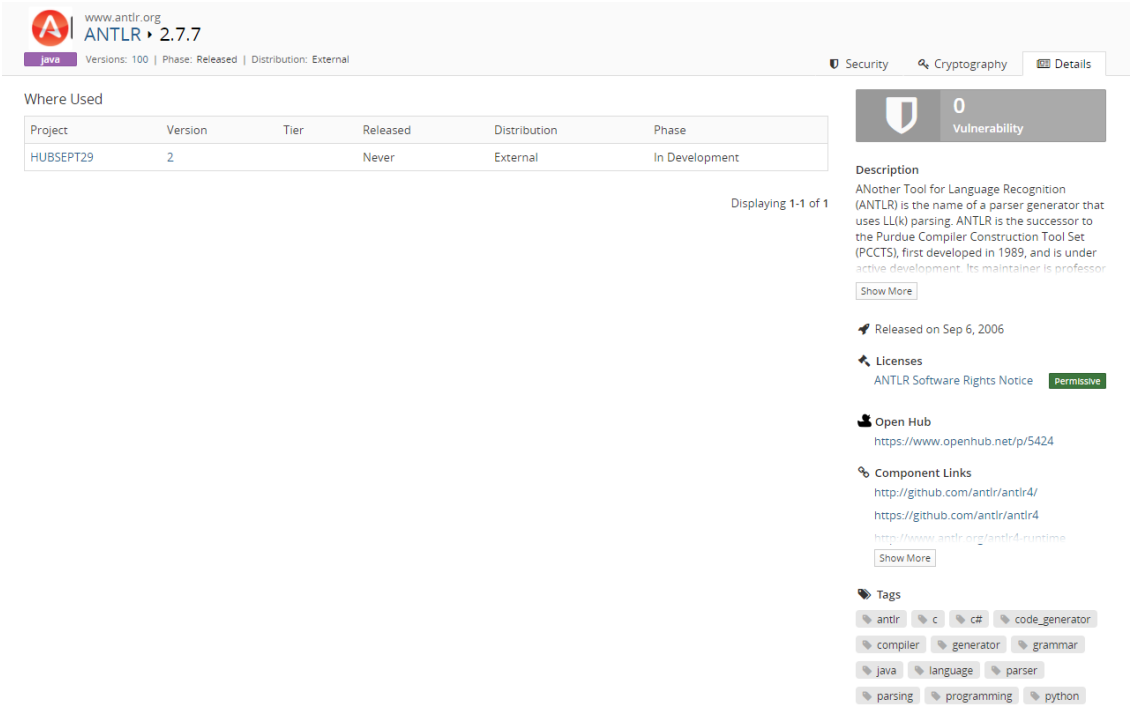
For components that have multiple versions, the total value equals the sum of all versions.

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:

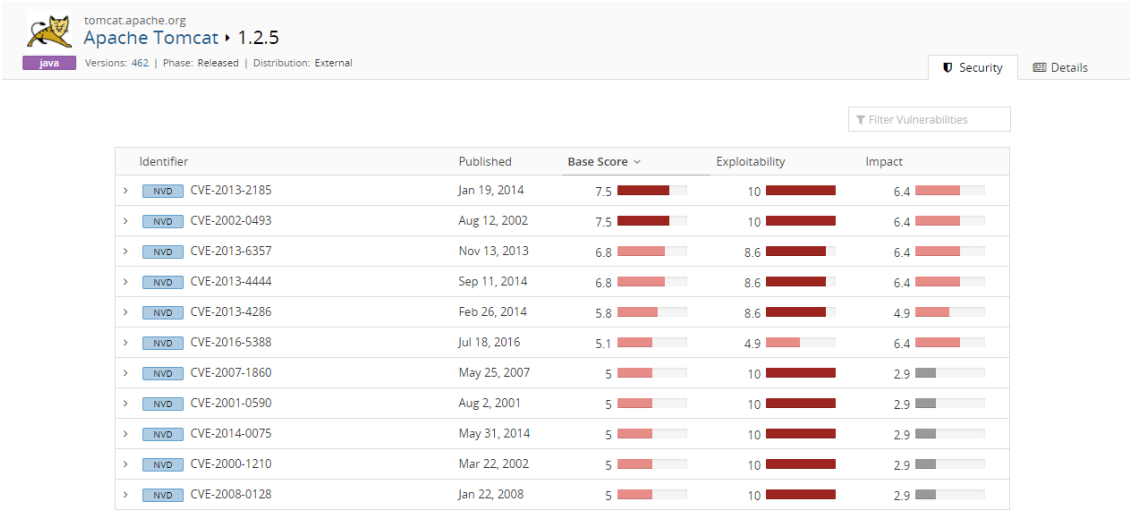


The **Used count** column shows the number of project versions that use this version of this component. A graph at the top of the page shows a history of high, medium, and low vulnerabilities for each version of this component.

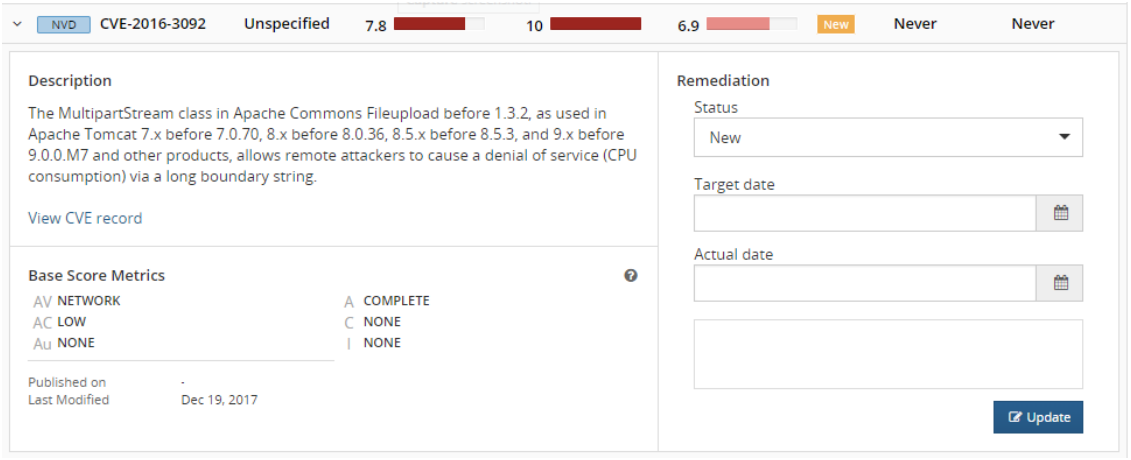
   - Select a component version to view a page which lists all projects and associated versions that use this version of this component. The number of vulnerabilities, a brief description, and associated licenses with this project also appear on this page.



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



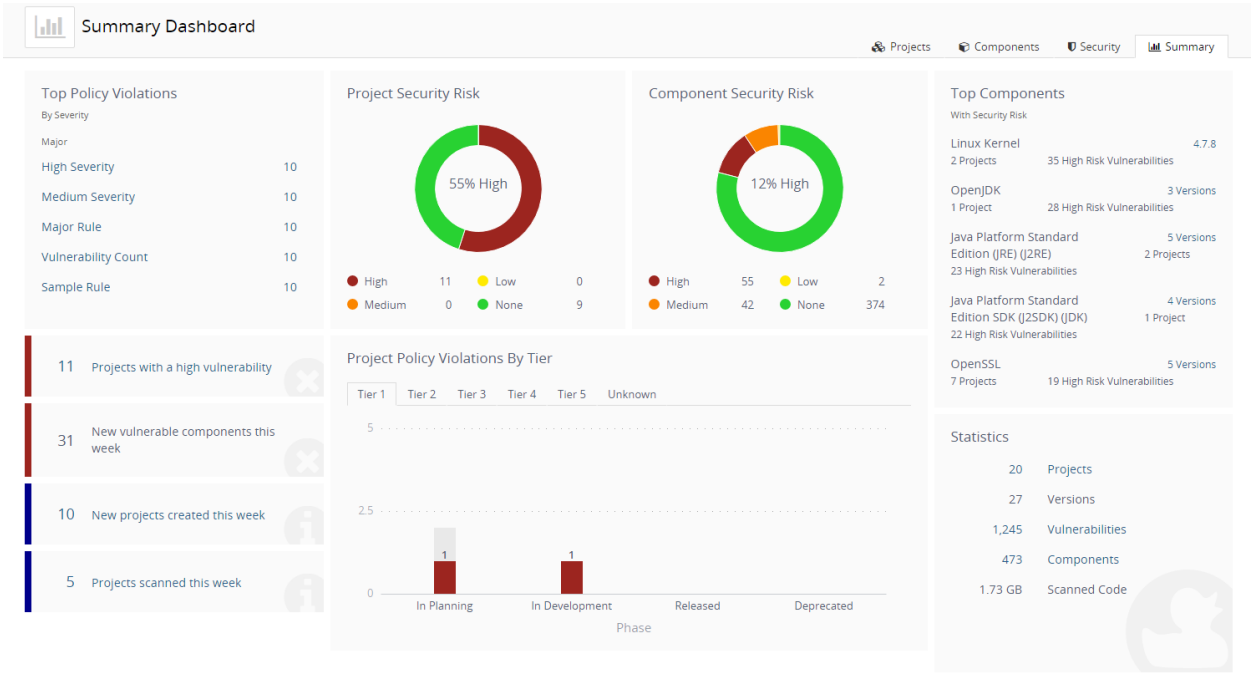
Click **>** to view more information on a vulnerability.



Select the link shown to view more information. Users with the BOM 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.

Description	More Information
The **New vulnerable components this week** widget displays the number of components the Black Duck KB mapped a vulnerability to in the past seven days, including today.	N/A.
The **New projects created this week** widget displays the number of projects that you have permission to view that have been created in the past seven days, including today.	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.