Getting Started

Black Duck SCA 2025.4.1

29-05-2025

Contents

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/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.

What is Black Duck SCA?

Black Duck SCA is a Software Composition Analysis (SCA) solution that helps organizations identify, track and manage open-source components in their codebase. It provides automated license compliance, security vulnerability detection, and risk assessment to help teams ensure the security and integrity of their software.

Key capabilities

- **Open source management**: Identify and track open-source components in your projects.
- **Vulnerability detection**: Automatically scan for security vulnerabilities using the National Vulnerability Database (NVD) and Black Duck Security Advisories (BDSA).

- **License compliance**: Analyze open-source licenses and ensure compliance with corporate policies.
- **Risk assessment & policy enforcement**: Define and enforce policies to mitigate security, legal, and operational risks.
- **Software bill of materials (SBOM) generation**: Produce and manage SBOMs to maintain transparency over software dependencies.

How does Black Duck SCA work?

- **Scan your code**: Use Black Duck scanning tools (Detect, integrations, or APIs) to analyze your codebase.
- **Identify components**: Black Duck maps your code's dependencies to known open-source libraries in its KnowledgeBase (KB).
- **Assess risks**: Black Duck checks for security vulnerabilities, license issues, and policy violations.
- **Take action**: View reports, prioritize risks, apply remediations, and generate SBOMs for compliance.

How do you get started?

1. **Set up an account**: Log in to your Black Duck instance or cloud-hosted environment.
2. **Run your first scan**: Analyze a sample project and review the findings.
3. **Review results**: Explore vulnerabilities, license risks, and policy violations in the UI.

Start exploring Black Duck SCA

- How to perform a scan using Detect
- Understanding vulnerability reports
- Managing policy violations
- Generating a SBOM

Next steps

Once you're familiar with the basics, dive deeper into Black Duck's advanced features and technical configurations with the following Community resources:

- Navigating the Interface
- Working with Scan Results
- A Technical Introduction to Black Duck
- **Learn more**: Access documentation and training resources.

2. Logging in to Black Duck

To access Black Duck SCA, you need to log in through your browser. Logging in gives you access to project data, including projects that may be restricted to your team and organization.

Note: You must have valid login credentials. If you do not have a username or password, contact your Black Duck administrator.

Login options

Depending on how your organization has configured authentication, you may be able to log in using:

- Local Black Duck credentials: A username and password created by your administrator.
- LDAP credentials: Your organization's directory service login (if LDAP is enabled).
- SAML-based single sign-on (SSO): You may be directed to your company's login provider (if SAML is configured).

Note: If Multi-Factor Authentication (MFA) is enabled, it only applies to users logging in with local credentials. Users authenticating through SAML or LDAP will not be prompted for MFA.

If you're unsure which method applies to you, reach out to your administrator for guidance.

Steps to log in

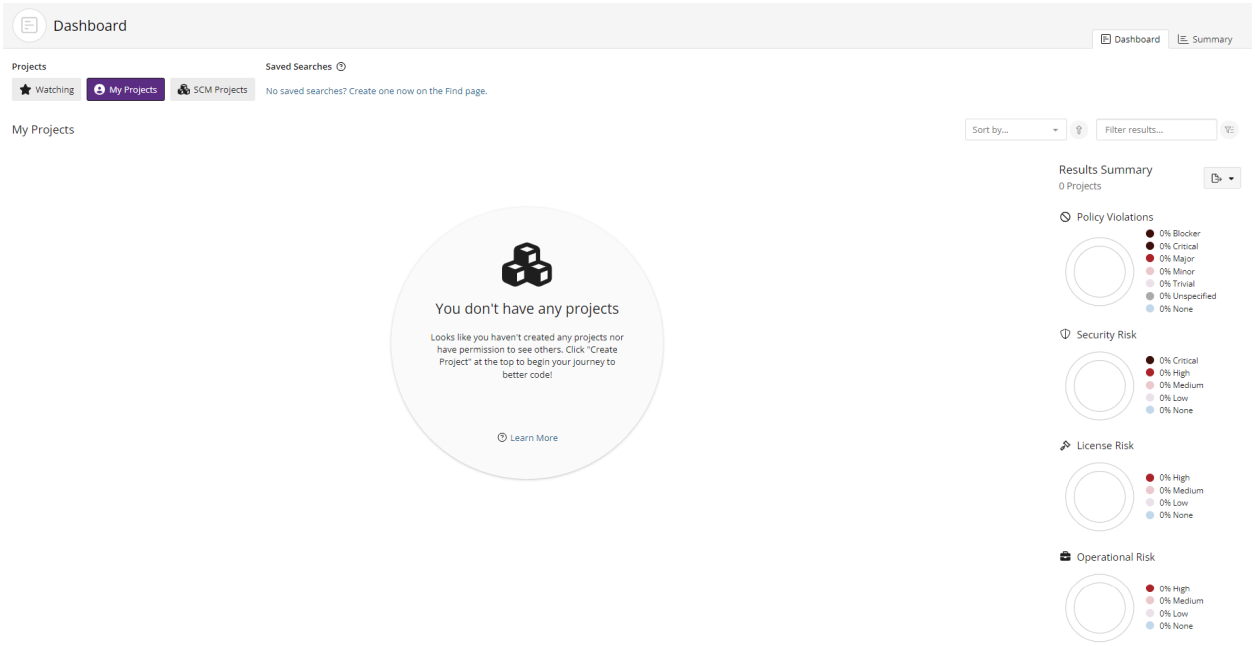
1. Open a browser and navigate to the Black Duck URL provided by your system administrator. The URL typically follows this format:

   ```
   https://<your-black-duck-server-hostname>
   ```

2. Enter your username and password.
   - Passwords are case-sensitive.
   - If this is your first login or your password doesn't meet the system's security requirements, you'll be prompted to change it. Follow the on-screen password rules to complete the update.
3. Click **Login**.
4. If MFA is enabled on your instance, you'll be prompted to configure it the first time you log in:
   - A QR code will be displayed.
   - Use a supported authentication app (such as Google Authenticator) to scan the QR code.
   - Enter the 6-digit code from your app to complete the setup.

After logging in

On your first login, you'll land on an empty Dashboard.



To populate your dashboard with data, you need to scan your code and map it to a project version. These steps are covered in the next section of this guide.

By default, the Dashboard shows:

- My Projects: Projects you've created or been assigned to.
- Watching: Projects or components you've marked to monitor.

You can also create custom dashboards by saving searches for specific projects, versions, or components you care about. Saved searches will appear on your Dashboard for quick access.

3. Scanning your code

Scanning is the core way Black Duck identifies open source components, licenses, and known vulnerabilities in your codebase. When you run a scan, Black Duck analyzes your project files and generates a comprehensive Bill of Materials (BOM), helping you stay compliant, secure, and informed.

What does a Black Duck scan do?

Black Duck scans your codebase to:

- Identify open source components and their versions
- Detect known security vulnerabilities using sources like the National Vulnerability Database (NVD) and Black Duck Security Advisories (BDSA)
- Evaluate license risk and compliance
- Generate a BOM for auditing and reporting
- Enforce custom policies based on your organization's risk tolerance

Scans can be triggered during development, in CI/CD pipelines, or manually—depending on how you choose to integrate Black Duck.

Available scanning tools

Black Duck offers a variety of tools to suit different environments and workflows:

- Black Duck Detect (CLI): A flexible command-line tool that supports scanning source code, binaries, and containers. Can be integrated into local development or CI/CD pipelines. Black Duck Detect is the recommended scanning tool for Black Duck.
- Signature Scanner (CLI): A dedicated command-line tool for running signature-based scans. Best suited for environments where Detect is not ideal or where direct control over scan configuration is required.
- Black Duck plugin integrations: Prebuilt integrations for popular tools like:
  - Jenkins
  - Azure DevOps
  - GitHub Actions
  - Bitbucket Pipelines
- SCA Scan Service (SCASS): A scalable cloud-based scanning service for source, binary, and container analysis. Available for customers with the appropriate license.
- REST API: Advanced users can use the Black Duck API to automate scan uploads, retrieve results, and manage project data.

Note: Some features may require a specific license or configuration. Contact your administrator if you are unsure which scanning tools are available in your environment.

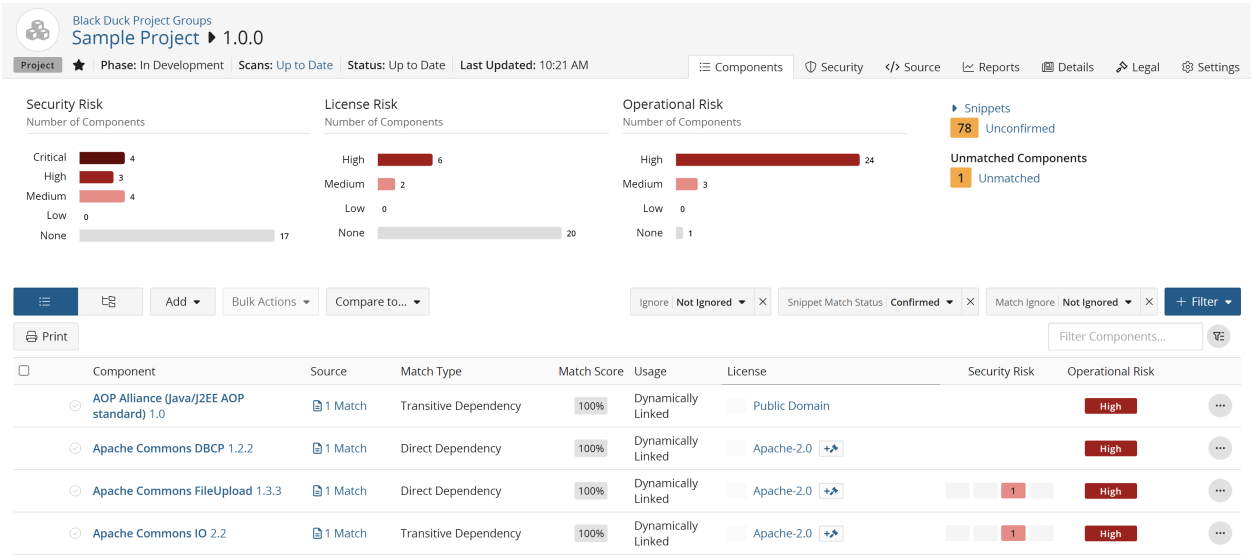
4. Viewing your Bill of Materials (BOM)

Once you have scanned your codebase and mapped the results to a project version, Black Duck automatically generates a Bill of Materials (BOM). The BOM lists all the open source components detected in that project version, along with associated data like licenses, vulnerabilities, and policy status.

The BOM is your central view for understanding what's in your software and whether any risks or compliance issues need to be addressed.

How to view a BOM

1. Log in to Black Duck.
2. On the **Dashboard**, select the project using either the **Watching** or My Projects tab.
3. On the **Project** page, choose the version you want to view. This will take you to the **Components** tab, which displays the BOM.



Understanding the BOM view

- The BOM shows all open source components found in the selected project version.
- By default, it dispalys a flat view, meaning all components appear in a single list, regardless of how they were introduced into the codebase.
- Each component entry includes important details such as the component's name and version, match type, license(s), and security and operational risks. Click here for more information on these component characteristics.

You can sort, filter, and search within the BOM to focus on components that are high-risk or policy-violating.

What you can do from the BOM

- Click a component to open a slide-out panel with more detailed information, including:
  - Vulnerabilities
  - Licenses

  - Origin IDs (e.g., PURL, CPE)
  - Other details, such as description and approval status
- Apply policy overrides or remediation actions directly from the BOM if you have the appropriate permissions.
- Generate an SBOM report using supported formats such as SPDX or CycloneDX.

Deeper dive

- To explore what you can do with the BOM, see Project Version BOMs in the Black Duck documentation.
- For help interpreting vulnerabilities, see Managing Security Risk.
- To learn about setting policies, see Managing Policies.