



入门

Black Duck SCA 2025.4.0

Black Duck 版权所有 ©2025。

保留所有权利。本文档的所有使用均受 Black Duck Software, Inc. 和被许可人之间的许可协议约束。未经 Black Duck Software, Inc. 事先书面许可，不得以任何形式或任何方式复制或传播本文档的任何内容。

Black Duck、Know Your Code 和 Black Duck 徽标是 Black Duck Software, Inc. 在美国和其他司法管辖区的注册商标。Black Duck Code Center、Black Duck Code Sight、Black Duck Hub、Black Duck Protex 和 Black Duck Suite 是 Black Duck Software, Inc. 的商标。所有其他商标或注册商标是其各自所有者的专有财产。

02-10-2025

内容

- 前言..... 4
 - Black Duck 文档..... 4
 - 客户支持..... 4
 - Black Duck 社区..... 5
 - 培训..... 5
 - Black Duck 关于包容性和多样性的声明..... 5
 - Black Duck 安全承诺..... 5
- 1. 关于 Black Duck..... 7
- 2. 登录到 Black Duck..... 9
- 3. 扫描您的代码..... 11
- 4. 查看材料清单 (BOM)..... 12

前言

Black Duck 文档

Black Duck 的文档包括在线帮助和以下文档：

标题	文件	说明
发行说明	release_notes.pdf	包含与当前版本和先前版本中的新功能和改进功能、已解决问题和已知问题有关的信息。
使用 Docker Swarm 安装 Black Duck	install_swarm.pdf	包含有关使用 Docker Swarm 安装和升级 Black Duck 的信息。
使用 Kubernetes 安装 Black Duck	install_kubernetes.pdf	包含有关使用 Kubernetes 安装和升级 Black Duck 的信息。
使用 OpenShift 安装 Black Duck	install_openshift.pdf	包含有关使用 OpenShift 安装和升级 Black Duck 的信息。
入门	getting_started.pdf	为初次使用的用户提供了有关使用 Black Duck 的信息。
扫描最佳做法	scanning_best_practices.pdf	提供扫描的最佳做法。
SDK 入门	getting_started_sdk.pdf	包含概述信息和样本使用案例。
报告数据库	report_db.pdf	包含有关使用报告数据库的信息。
用户指南	user_guide.pdf	包含有关使用 Black Duck 的 UI 的信息。

在 Kubernetes 或 OpenShift 环境中安装 Black Duck 软件的安装方法是 Helm。单击以下链接查看文档。

- [Helm](#) 是 Kubernetes 的软件包管理器，可用于安装 Black Duck。Black Duck 支持 Helm3，Kubernetes 的最低版本为 1.13。

Black Duck 集成文档位置：

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

客户支持

如果您在软件或文档方面遇到任何问题，请联系 Black Duck 客户支持：

- 在线：<https://community.blackduck.com/s/contactsupport>
- 要创建支持案例，请登录 Black Duck Community 网站：<https://community.blackduck.com/s/contactsupport>。
- 另一个可随时使用的方便资源是[在线社区门户](#)。

Black Duck 社区

Black Duck 社区是我们提供客户支持、解决方案和信息的主要在线资源。该社区允许用户快速轻松地打开支持案例，监控进度，了解重要产品信息，搜索知识库，以及从其他 Black Duck 客户那里获得见解。社区中包含的许多功能侧重于以下协作操作：

- 连接 - 打开支持案例并监控其进度，以及监控需要工程或产品管理部门协助的问题
- 学习 - 其他 Black Duck 产品用户的见解和最佳做法，使您能够从各种行业领先的公司那里汲取宝贵的经验教训。此外，客户中心还允许您轻松访问 Black Duck 的所有最新产品新闻和动态，帮助您更好地利用我们的产品和服务，最大限度地提高开源组件在您的组织中的价值。
- 解决方案 - 通过访问 Black Duck 专家和我们的知识库提供的丰富内容和产品知识，快速轻松地获得您正在寻求的答案。
- 分享 - 与 Black Duck 员工和其他客户协作并进行沟通，以众包解决方案，并分享您对产品方向的想法。

[访问客户成功社区](#)。如果您没有帐户或在访问系统时遇到问题，请单击[此处](#)开始，或发送电子邮件至 community.manager@blackduck.com。

培训


Black Duck “客户教育”是满足您所有 Black Duck 教育需求的一站式资源。它使您可以全天候访问在线培训课程和操作方法视频。

每月都会添加新视频和课程。

在 Black Duck 教育，您可以：

- 按照自己的节奏学习。
- 按照您希望的频率回顾课程。
- 进行评估以测试您的技能。
- 打印完成证书以展示您的成就。

要了解更多信息，请访问 <https://blackduck.skilljar.com/page/black-duck>，或者，要获取 Black Duck 的帮助

信息，请选择 Black Duck 教程（从“帮助”菜单 （位于 Black Duck UI 中）选择）。

Black Duck 关于包容性和多样性的声明

Black Duck 致力于打造一个包容性的环境，让每位员工、客户和合作伙伴都感到宾至如归。我们正在审查并移除产品中的排他性语言以及支持面向客户的宣传材料。我们的举措还包括通过内部计划从我们的工程和工作环境中移除偏见语言（包括嵌入我们软件和 IP 中的术语）。同时，我们正在努力确保我们的 Web 内容和软件应用程序可供不同能力的人使用。由于我们的 IP 实施了行业标准规范，目前正在审查这些规范以移除排他性语言，因此您可能仍在我们的软件或文档中找到非包容性语言的示例。

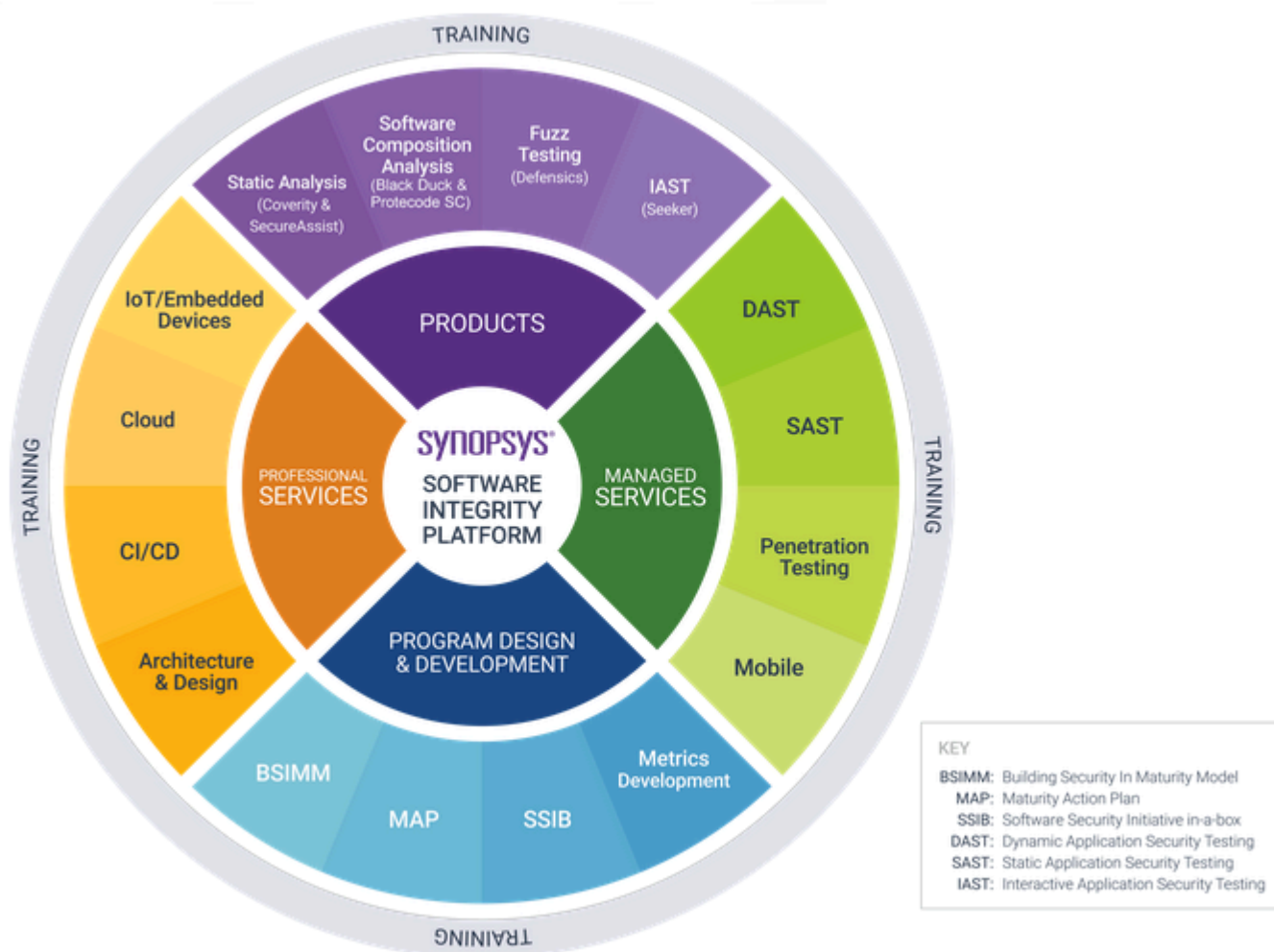
Black Duck 安全承诺

作为一家致力于保护和保障客户应用程序安全的组织，Black Duck 同样致力于客户的数据安全和隐私。本声明旨在为 Black Duck 客户和潜在客户关于我们的系统、合规性认证、流程和其他安全相关活动的最新信息。

本声明可在以下位置获取：[安全承诺 | Black Duck](#)

1. 关于 Black Duck

Black Duck 提供全面的服务和工具套件，为客户的安全之旅提供支持。从刚开始接触安全领域的客户，到正在加强其现有计划的客户，Black Duck 都可以提供成功所需的专业知识、技能和产品。



什么是 Black Duck SCA ？

Black Duck SCA 是一种软件构成分析 (SCA) 解决方案，可帮助组织识别、跟踪和管理其代码库中的开源组件。它提供自动化许可证合规、安全漏洞检测和风险评估，帮助团队确保其软件的安全性和完整性。

关键功能

- 开源管理：识别并跟踪项目中的开源组件。
- 漏洞检测：使用国家漏洞数据库 (NVD) 和 Black Duck 安全公告 (BDSA) 自动扫描安全漏洞。
- 许可证合规：分析开源许可证，确保符合公司政策。
- 风险评估和策略执行：定义并执行策略，以降低安全、法律和运维风险。

1. 关于 Black Duck •

- 软件材料清单 (SBOM) 生成：生成和管理 SBOM，以保持软件依赖关系的透明度。

Black Duck SCA 如何工作？

- 扫描您的代码：使用 Black Duck 扫描工具（Detect、集成或 API）分析您的代码库。
- 识别组件：Black Duck 将您的代码依赖关系映射到其 KnowledgeBase (KB) 中的已知开源库。
- 评估风险：Black Duck 会检查安全漏洞、许可证问题和策略违反。
- 采取行动：查看报告、确定风险优先级、应用修复并生成 SBOM 以确保合规。

如何开始？

1. [设置一个帐户](#)：登录您的 Black Duck 实例或云托管环境。
2. [运行第一次扫描](#)：分析样本项目并查看发现结果。
3. [查看结果](#)：在 UI 中发现漏洞、许可证风险和策略违规。

开始探索 Black Duck SCA

- [如何使用 Detect 执行扫描](#)
- [了解漏洞报告](#)
- [管理策略违规](#)
- [生成 SBOM](#)


后续步骤

熟悉基础知识后，请使用以下社区资源深入了解 Black Duck 的高级功能和技术配置：

- [浏览界面](#)
- [使用扫描结果](#)
- [Black Duck 技术介绍](#)
- 了解更多：访问[文档](#)和[培训](#)资源。

2. 登录到 Black Duck


要访问 Black Duck SCA，您需要通过浏览器登录。登录后，您将有权访问项目数据，包括可能仅限于团队和组织访问的项目。

 注：您必须拥有有效的登录凭据。如果没有用户名或密码，请联系 Black Duck 管理员。

登录选项

取决于您的组织如何配置身份验证，您可以使用以下方式登录：

- 本地 Black Duck 凭据：由管理员创建的用户名和密码。
- LDAP 凭据：组织的目录服务登录（如果已启用 LDAP）。
- 基于 SAML 的单点登录 (SSO)：您可能会被引导到公司的登录提供商处（如果已配置 SAML）。

 注：如果启用了多因素身份验证 (MFA)，它只适用于使用本地凭据登录的用户。通过 SAML 或 LDAP 进行身份验证的用户不会收到 MFA 提示。

如果您不确定哪种方法适用于您，请与您的管理员联系，以获取指导。

登录步骤

1. 打开浏览器，导航到系统管理员提供的 Black Duck URL。该 URL 通常采用以下格式：

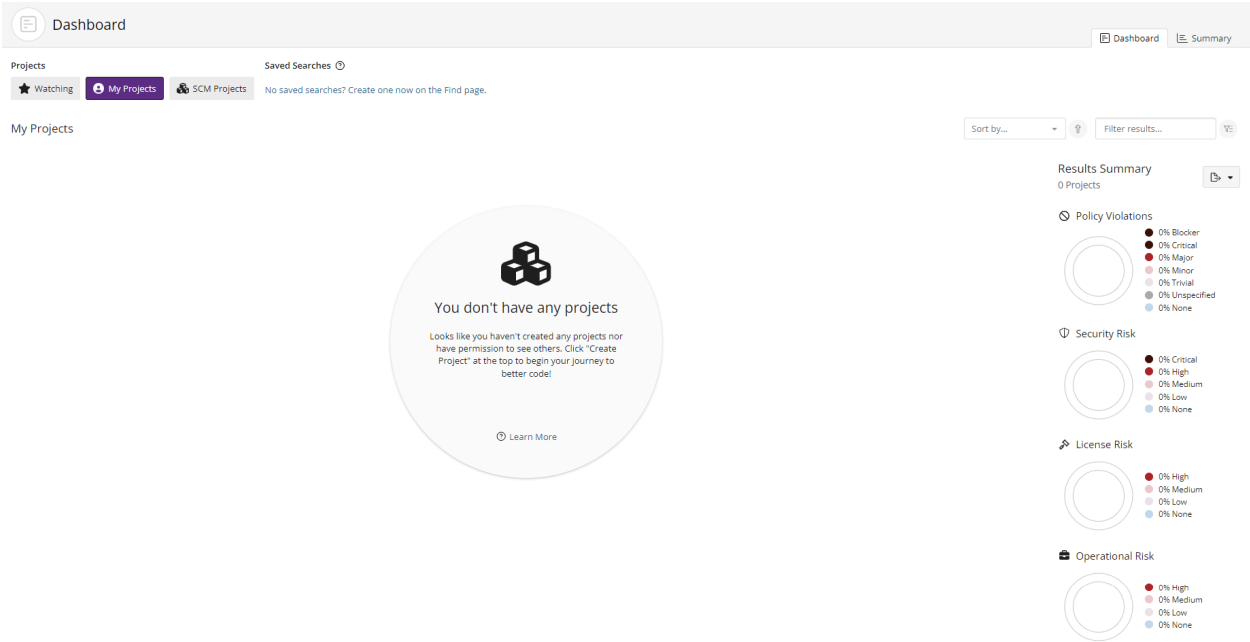
```
https://<your-black-duck-server-hostname>
```

2. 输入用户名和密码。
 - 密码区分大小写。
 - 如果这是您第一次登录，或密码不符合系统的安全要求，系统会提示您更改密码。按照屏幕上的密码规则完成更新。
3. 单击登录。
4. 如果您的实例已启用 MFA，在首次登录时，您会收到[对其进行配置](#)的提示：
 - 会显示一个二维码。
 - 使用受支持的身份验证应用程序（如 Google Authenticator）扫描二维码。
 - 输入应用程序中的 6 位数字代码，完成设置。

登录后

第一次登录时，您将进入空的仪表板。

2. 登录到 Black Duck •



要在仪表板上填充数据，需要[扫描代码并将其映射到项目版本](#)。本指南的下一部分将涵盖这些步骤。

默认情况下，仪表板显示：

- 我的项目：您创建或被分配的项目。
- 观察：您标记为要监控的项目或组件。

对于您关注的特定项目、版本或组件，您还可以通过保存对它们搜索，创建[自定义仪表板](#)。保存的搜索将显示在仪表板上，以便快速访问。

3. 扫描您的代码

扫描是 Black Duck 识别代码库中开源组件、许可证和已知漏洞的核心方法。运行扫描时，Black Duck 会分析您的项目文件并生成一份全面的材料清单 (BOM)，帮助您保持合规、安全和知情。

Black Duck 扫描有哪些作用？

Black Duck 扫描您的代码库，以：


- 识别开源组件及其版本
- 使用国家漏洞数据库 (NVD) 和 Black Duck 安全公告 (BDSA) 等来源检测已知的安全漏洞
- 评估许可证风险和合规性
- 生成用于审计和报告的 BOM
- 根据您组织的风险承受能力执行自定义策略

扫描可以在开发过程中、CI/CD 管道中触发，也可手动触发，具体取决于您集成 Black Duck 的方式。

可用的扫描工具

Black Duck 提供各种工具，以适应不同的环境和工作流程：

- [Black Duck Detect \(CLI\)](#)：灵活的命令行工具，支持扫描源代码、二进制文件和容器。可以集成到本地开发或 CI/CD 管道中。Black Duck Detect 是推荐用于 Black Duck 的扫描工具。
- [特征扫描程序 \(CLI\)](#)：专用的命令行工具，用于运行基于特征的扫描。最适合 Detect 不是理想选择或需要对扫描配置进行直接控制的环境。
- [Black Duck 插件集成](#)：针对热门工具预构建的集成，例如：
 - Jenkins
 - Azure DevOps
 - GitHub Actions
 - Bitbucket Pipelines
- [SCA 扫描服务 \(SCASS\)](#)：基于云的可扩展扫描服务，适用于源、二进制文件和容器分析。具有相应许可证的客户均可使用。
- [REST API](#)：高级用户可使用 Black Duck API 自动上传扫描、检索结果和管理项目数据。

 注：某些功能可能需要特定的许可证或配置。如果您不确定您的环境中可以使用哪些扫描工具，请联系您的管理员。

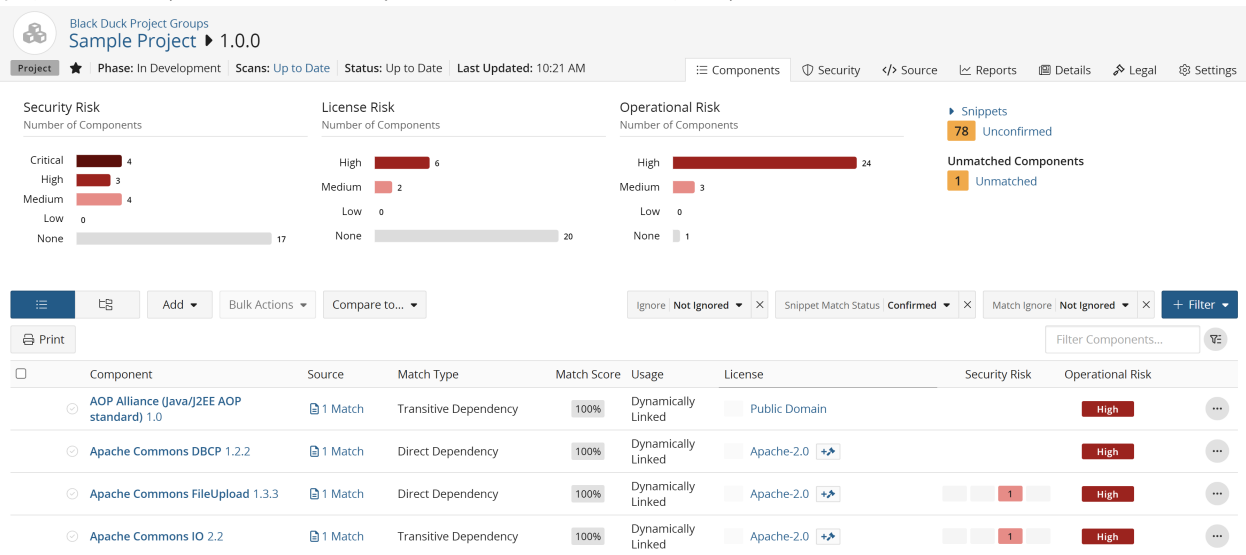
4. 查看材料清单 (BOM)

扫描代码库并将结果映射到项目版本后，Black Duck 会自动生成材料清单 (BOM)。BOM 会列出该项目版本中检测到的所有开源组件，以及许可证、漏洞和策略状态等相关数据。

BOM 让您可以在一个核心视图中了解软件所包含的内容，以及是否需要处理任何风险或合规问题。

如何查看 BOM

1. 登录 Black Duck。
2. 在仪表板上，使用正在关注或我的项目选项卡选择项目。
3. 在项目页面上，选择要查看的版本。这将带您进入组件选项卡，其中将显示 BOM。



了解 BOM 视图

- BOM 会显示在所选项目版本中找到的所有开源组件。
- 默认情况下，它显示扁平视图，即在单一列表中显示所有组件（无论将它们引入代码库的方法是什么）。
- 每个组件条目都包含重要的详细信息，例如组件的名称和版本、匹配类型、许可证，以及安全和运维风险。单击[此处](#)了解有关这些组件特征的更多信息。

您可以在 BOM 中进行排序、过滤和搜索，以关注存在高风险或策略违规的组件。

在 BOM 中可以进行的操作

- 单击组件将打开滑出面板，其中包含更多详细信息，包括：
 - 漏洞
 - 许可证
 - 来源 ID（如 PURL、CPE）
 - 其他详细信息，如描述和批准状态
- 如果有适当的权限，您可以直接从 BOM [应用策略覆盖](#)或[修复](#)操作。

- 使用 SPDX 或 CycloneDX 等受支持的格式[生成 SBOM 报告](#)。

深入探讨

- 要探索 BOM 的用途，请参阅 [Black Duck 文档](#) 中的项目版本 BOM。
- 如需帮助解读漏洞，请参阅[管理安全风险](#)。
- 如需了解如何设置策略，请参阅[管理策略](#)。