SYNOPSYS®

入门

Black Duck 2023.4.0

内容

前言 3
Black Duck 文档 3
客户支持 3
Synopsys Software Integrity 社区 4
培训 4
Synopsys 关于包容性和多样性的声明 4

1. 关于 Black Duck 5

2. 登录 Black Duck 6

3. 扫描您的代码 8
使用 Synopsys Detect (Desktop) 8
创建项目 22
将扫描映射到项目 25

4. 查看 中的风险 Black Duck 28
仪表板 28
项目版本页面 33
查看仪表板 33
查看项目的运行状况 46
关于安全风险 51
安全风险级别 51
估计安全风险 51
建议的工作流程 52

5. 查看您的 BOM 53
在 BOM 中调整组件和/或组件版本 53

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。
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 Synopsysctl 和 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。
- Synopsysctl 是一款云原生管理命令行工具，用于在 Kubernetes 和 Red Hat OpenShift 中部署 Black Duck 软件。

Black Duck 集成文档可在 Confluence 上找到。

客户支持

如果您在软件或文档方面遇到任何问题，请联系 Synopsys 客户支持。

您可以通过以下几种方式联系 Synopsys 支持：

- 在线：https://www.synopsys.com/software-integrity/support.html
- 电话：请参阅我们的支持页面底部的“联系我们”部分以查找您当地的电话号码。

要打开支持案例，请登录 Synopsys Software Integrity 社区网站，网址为：https://community.synopsys.com/s/contactsupport。

另一个可随时使用的方便资源是在线客户门户。

Synopsys Software Integrity 社区

Synopsys Software Integrity 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 Software Integrity Group (SIG) 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 SIG 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 Synopsys 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 SIG 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 Software Integrity Group 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@synopsys.com。

培训

Synopsys Software Integrity 的客户教育 (SIG Edu) 板块是满足您的所有 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 Synopsys Software Integrity 的客户教育 (SIG Edu) 板块，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。

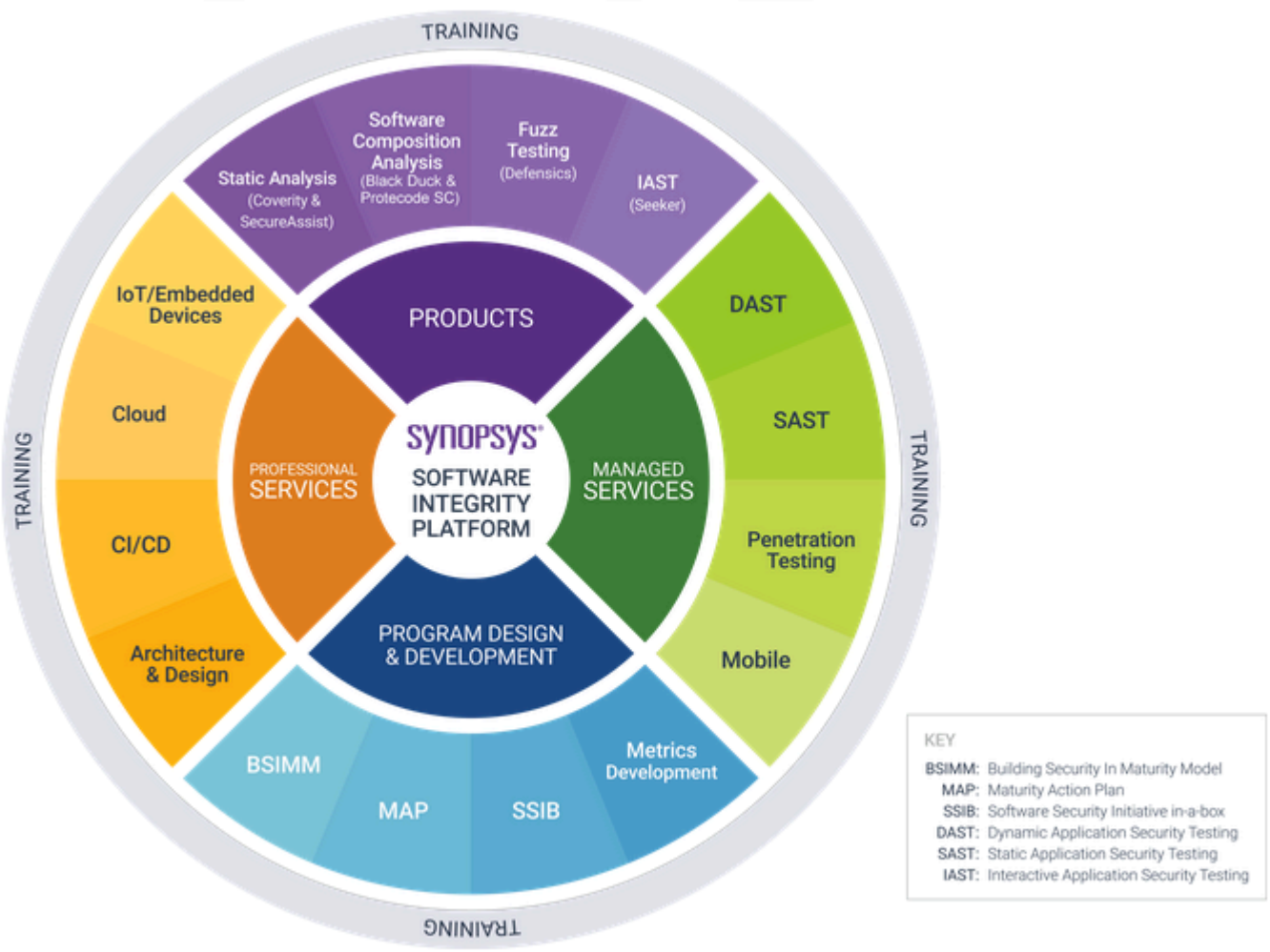
要了解更多信息，请访问 https://community.synopsys.com/s/education，或者，要获取 Black Duck 的帮助信息，请选择 Black Duck 教程（位于 Black Duck UI 的“帮助”菜单（ ）中）。

Synopsys 关于包容性和多样性的声明

Synopsys 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。

1. 关于 Black Duck

Synopsys Software Integrity Group (SIG) 提供了一套全面的服务和工具，可在客户的安全历程中为其提供支持。从刚开始筹备安全性的客户，到对成熟计划进行强化的客户，SIG 拥有取得成功所需的专业知识、技能和产品。



软件组成分析 (SCA) 工具 Black Duck 有助于管理软件供应链，了解使用中的第三方组件，并最大程度地降低已知漏洞和许可带来的风险。Black Duck 是一套全面的供应链管理解决方案，主要基于来源分析。

使用 Black Duck，您可以：

- 扫描代码并识别代码库中存在的开源软件。
- 查看为您的软件项目生成的材料清单 (BOM)。
- 查看已在开源组件中识别的漏洞。
- 评估您的安全性、许可证和操作风险。

2. 登录 Black Duck

登录 Black Duck 可让您搜索可能仅限于团队成员或公司员工的项目。

注: 您必须具有用户名和密码才能访问 Black Duck。如果您没有用户名，请与系统管理员联系。如果 Black Duck 配置为使用 LDAP，则可以使用这些凭据登录 Black Duck。

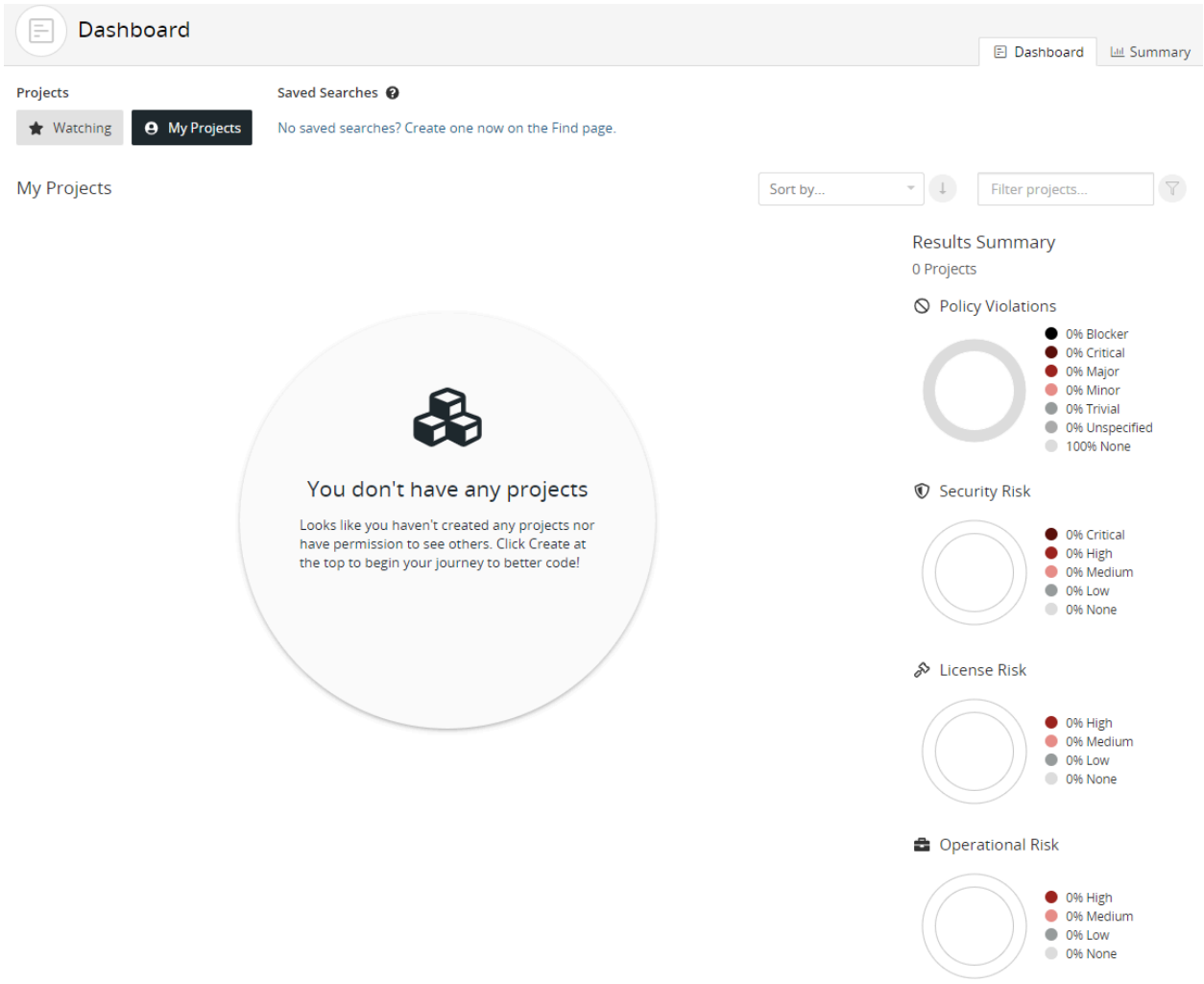
要登录 Black Duck：

1. 使用浏览器导航至系统管理员提供的 Black Duck URL。通常，URL 的格式为 https://<server hostname>。
2. 输入 Black Duck 管理员提供的用户名和密码。您的密码区分大小写。

   注: 如果您的管理员已启用密码要求，但您的密码不符合要求，则会出现一个对话框，通知您必须更改密码。更新密码时，请确保密码符合对话框中列出的要求。除非密码满足所有要求，否则您将无法登录到 Black Duck。

3. 单击登录。

   当您在安装 Black Duck 后首次登录时，将出现一个空“仪表板”页面。要在 Black Duck 中显示信息，您需要扫描代码并将代码映射到项目，如下一章所述。



默认情况下，“仪表板”页面仅显示正在关注和我的项目仪表板。您还可以创建自定义仪表板，以便快速查看对您至关重要的项目版本或组件版本：搜索项目和/或组件，然后保存搜索。您保存的搜索将显示在“仪表板”页面上。

3. 扫描您的代码

Black Duck 组件扫描是一种扫描功能，它提供了一种自动化方法来确定构成软件项目的开源软件 (OSS) 组件集。组件扫描通过识别和编目 OSS 组件来帮助组织管理开源二进制文件的使用，以便提供这些组件的许可证、漏洞和 OSS 项目运行状况等附加元数据。

Black Duck 提供以下扫描工具：

- Synopsys Detect。Synopsys Detect 是推荐用于 Black Duck 的扫描工具。
- Black Duck 的快速扫描为开发人员提供了一种方法，以快速确定项目中包含的开源组件版本是否违反了与使用开源组件有关的公司策略。通过使用 Synopsys Detect，快速扫描可以快速返回结果，因为它只使用软件包管理器扫描，并且不与 Black Duck 服务器数据库交互。有关快速扫描的详细信息，请参阅 Black Duck 在线帮助或用户指南。
- Synopsys Detect (Desktop)，如下所述。
- 特征扫描程序 的命令行 (CLI) 版本。有关详细信息，请参阅 Black Duck 在线帮助或用户指南。

使用 Synopsys Detect (Desktop)

Synopsys Detect (Desktop) 提供了一个新界面，使扫描代码变得更容易。

借助 Synopsys Detect (Desktop)，您可以：

- 扫描源目录、二进制文件和可执行文件以及 Docker 映像和发行版。
- 创建要在以后上传的扫描文件。
- 管理扫描文件。
- 将扫描文件直接上传到 Black Duck。
- 查看上传的扫描。

要使用 Synopsys Detect (Desktop)：

1. 下载并安装 Synopsys Detect (Desktop)。
2. 使用您的 Black Duck 服务器设置来配置 Synopsys Detect (Desktop) 并完成安装过程。
3. 使用 Synopsys Detect (Desktop) 来扫描和/或上传文件。

注：如果您超出扫描大小限制 (5 GB)（对于 Black Duck - 二进制分析 为 6 GB），则会显示一条错误消息。如果您收到此消息，请联系客户支持。

确保您的系统符合 Synopsys Detect 的系统要求。

- 单击此处了解最新版本的 Synopsys Detect 的系统要求。
- 单击此处查看以前版本的 Synopsys Detect 的文档。使用此页面查找 Synopsys Detect 版本并查看系统要求。

下载和安装 Synopsys Detect (Desktop)

1. 登录 Black Duck。
2. 导航至用户名下的下拉菜单，然后选择工具。

3. 在下载 Synopsys Detect (Desktop) 部分中选择要使用的操作系统，以从 Google Cloud Storage 下载可执行文件。
4. 运行可执行文件以安装 Synopsys Detect (Desktop)。

   如果要从 Synopsys Detect (Desktop) 的早期版本升级，则会出现一个选项，用于从早期版本迁移数据。

注: 当应用程序安装到与其名称相关的目录中时，Synopsys Detect (Desktop) 不会卸载以前版本的 Black Duck Detect Desktop。它也不会卸载安装在非默认目录中的 Synopsys Detect (Desktop) 版本。您必须手动卸载所有以前版本的 Black Duck Detect Desktop 和安装在非默认目录中的 Synopsys Detect (Desktop) 版本，并修复或删除任何快捷方式。

如果 Synopsys Detect (Desktop) 安装后未打开，则会显示以下错误信息：

```
The SUID sandbox helper binary was found, but is not configured correctly. Rather than
 run without sandboxing I'm aborting now. You need to make sure that /opt/Synopsys
 Detect/chrome-sandbox is owned by root and has mode 4755.
```

您的操作系统不在内核层支持沙盒。要在禁用沙盒的情况下运行 Synopsys Detect (Desktop)，请在命令行中输入以下内容：

```
synopsys-detect --no-sandbox
```

Windows 的命令行选项

- Synopsys Detect 的无人值守（静默）安装

  ```
  ./synopsys-detect-latest.exe /S
  ```

- 安装到特定目录

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

安装 Linux 版本的 Synopsys Detect (Desktop)

1. 从您的 Black Duck 服务器下载可执行文件，如上一节所述。
2. 安装 Synopsys Detect (Desktop)：

   ```
   cd Downloads
   ```

   要在 CentOS/RedHat 上安装：

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

   要在 Ubuntu/Debian 上安装：

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

3. 更改 chrome-sandbox 的权限：

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

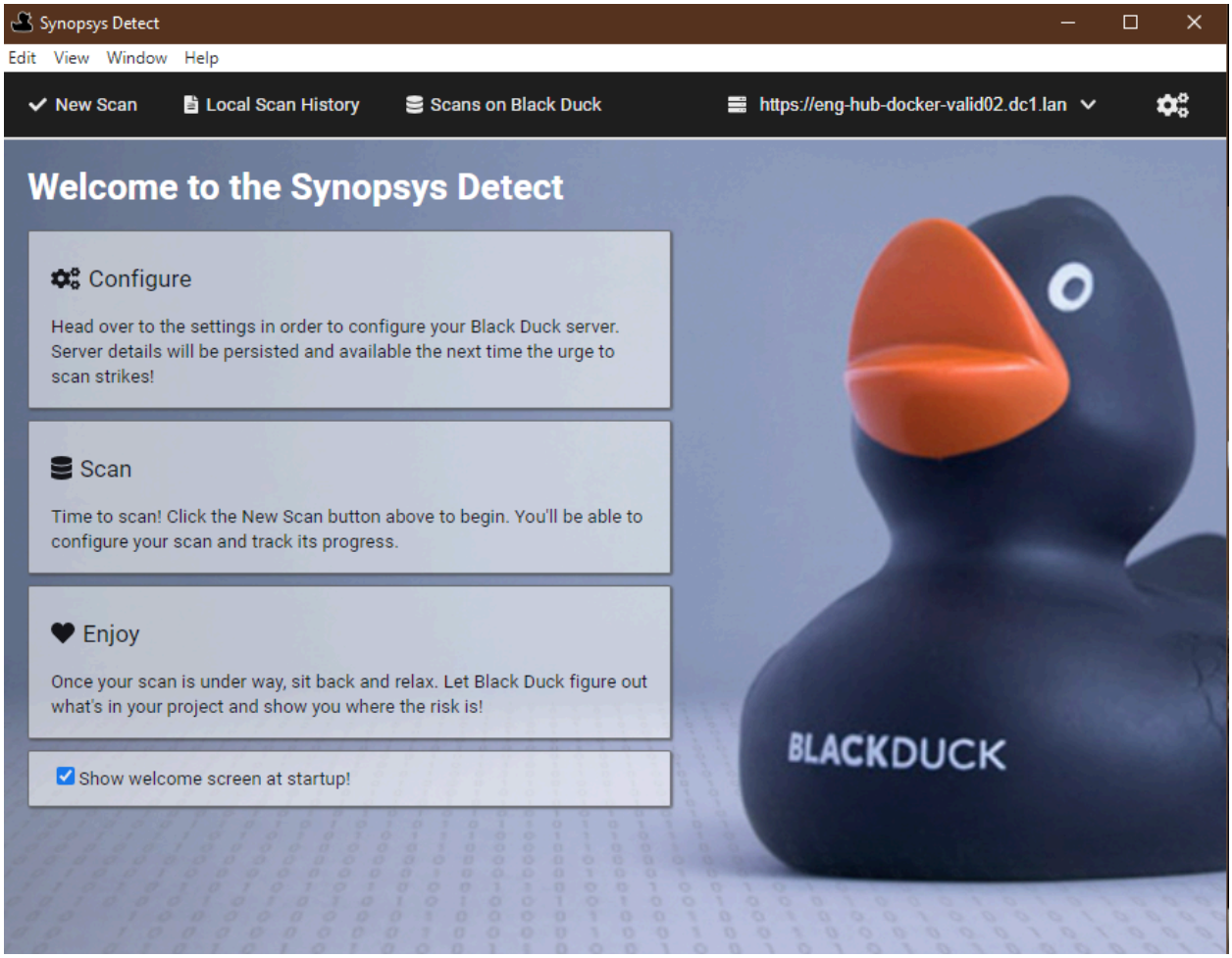
4. 运行 Synopsys Detect (Desktop)：

   ```
   ./synopsys-detect --no-sandbox
   ```

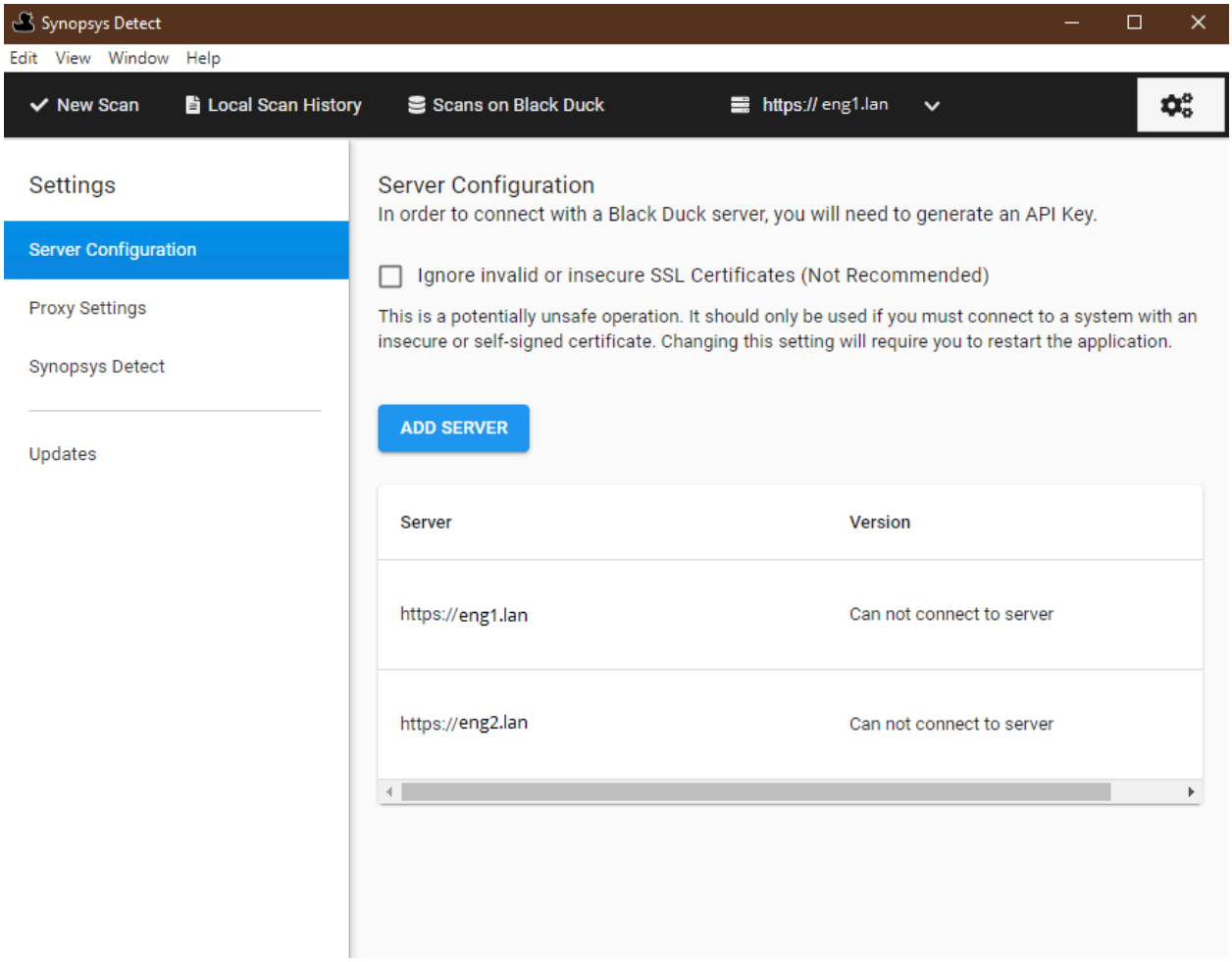
配置 Synopsys Detect (Desktop)

安装 Synopsys Detect (Desktop) 后，通过配置 Black Duck 设置继续安装过程。

1. 安装或升级到 Synopsys Detect (Desktop) 后，将显示“欢迎”页面。



2. 单击右上角的 将显示“设置”页面。



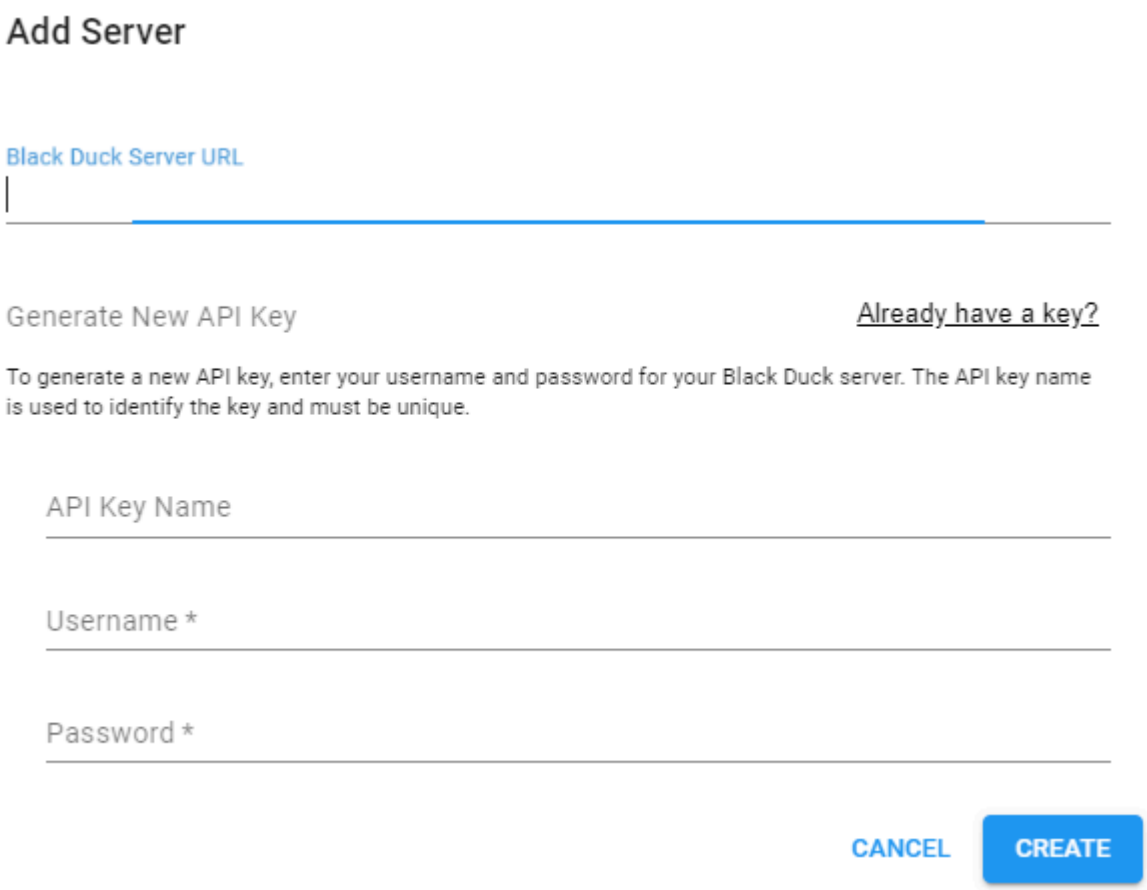
3. 如下所述，选择以下选项卡之一并完成安装和配置过程：
   - 服务器配置
   - 代理设置
   - Synopsys Detect
   - 更新

Black Duck 服务器配置

要添加服务器：

1. 选择服务器配置选项卡，然后单击添加服务器。

   将出现 “添加服务器” 对话框。



2. 指定 Black Duck 服务器 URL。像在浏览器中一样输入 Black Duck 服务器的 URL，例如 https://servername:8443/

   如果需要，请输入上下文信息，例如，如果在代理服务器/负载平衡器配置中指定了 X-Forwarded-Prefix 标头。

3. 生成或输入 API 密钥（用户访问令牌）。
   - 要生成新的 API 密钥：
     a. 输入密钥名称、用户名和密码。
     b. 单击创建。
   - 要输入 API 密钥：
     a. 选择已有密钥？。
     b. 在字段中输入 API 密钥。
     c. 单击创建。
4. 单击保存。 Synopsys Detect (Desktop) 连接到 Black Duck 服务器并显示连接到的 Black Duck 的版本。

要移除 API 密钥：

移除 API 密钥不会删除 Black Duck 中的密钥。此操作仅在本地移除密钥。

1. 选择服务器配置选项卡。
2. 单击服务器行中的 ⋮，然后选择移除 API 密钥。
   将出现“移除 API 密钥”对话框。
3. 单击确定以确认。

要删除配置

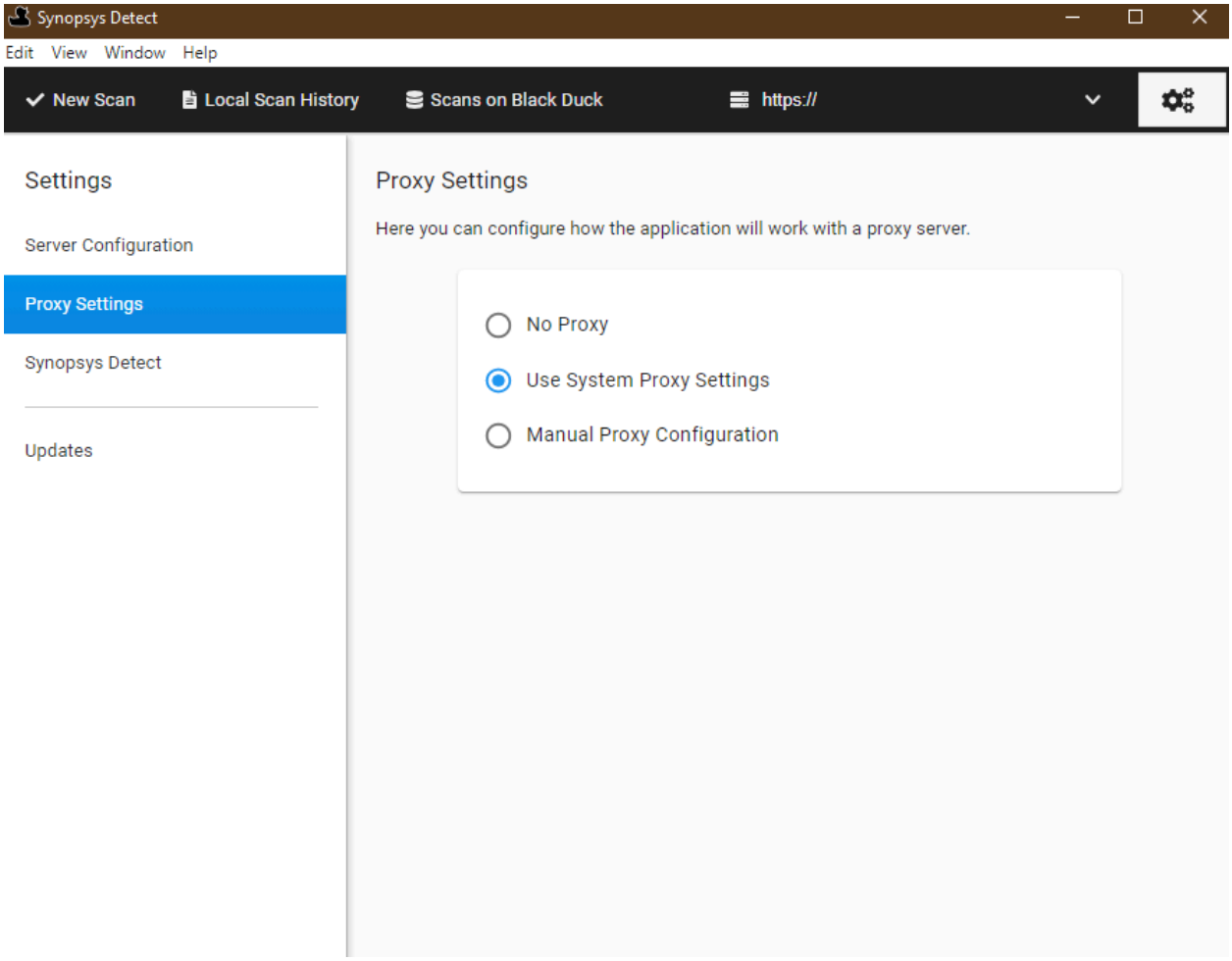
1. 单击服务器行中的 ⋮，然后选择删除配置。
   将出现“删除服务器配置”对话框。
2. 单击确定以确认。

代理设置

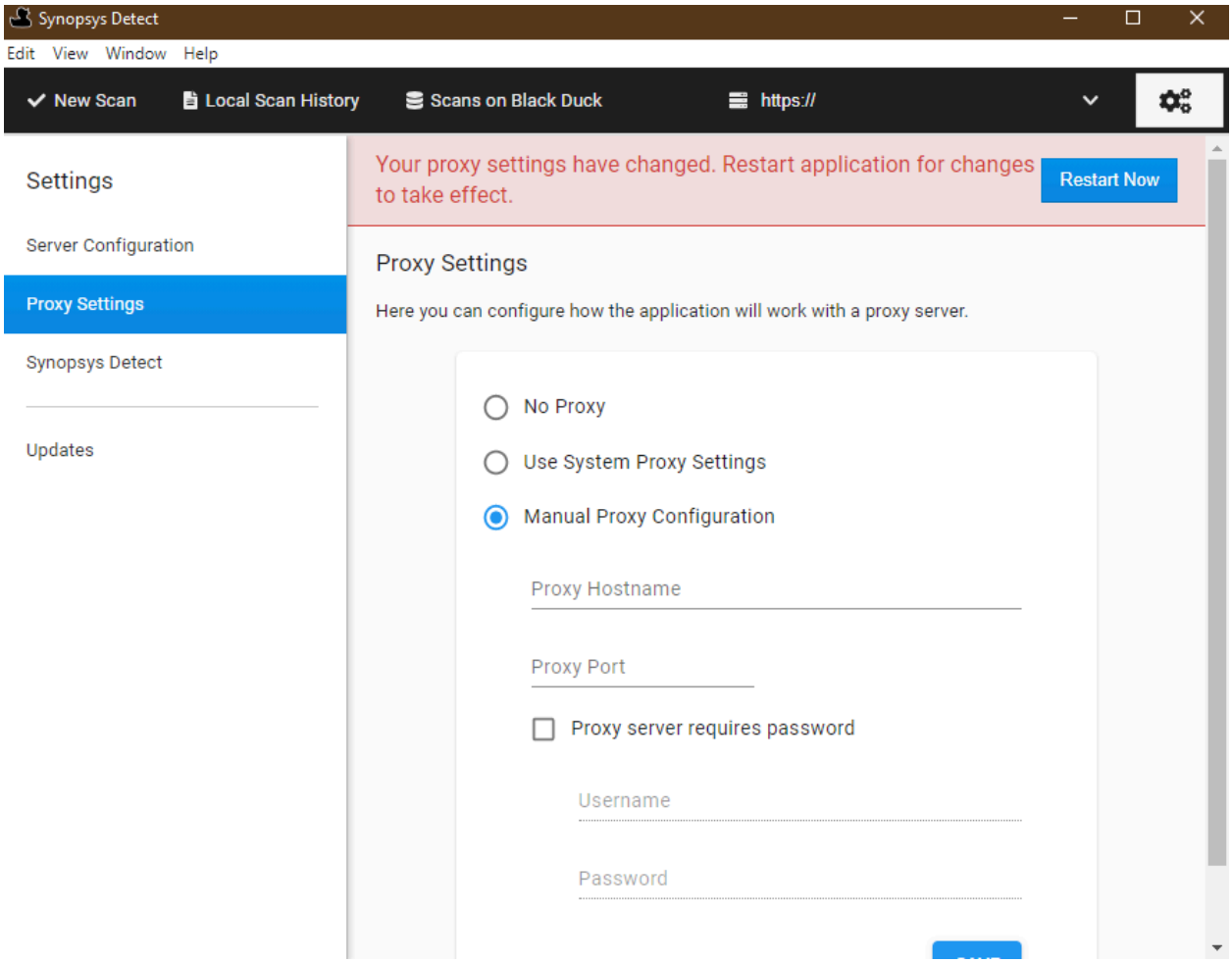
支持通过代理访问 Synopsys Detect (Desktop)。 Synopsys Detect (Desktop) 自动使用本地系统代理设置。如果需要手动输入代理设置或不需要代理，可以修改这些默认设置。

要修改默认代理设置：

1. 选择代理设置选项卡。



2. 选择无代理或手动代理配置。
3. 如果选择手动代理配置：



   a. 输入以下信息：
      - 您的代理主机名。
      - 端口号。
      - 是否需要身份验证。
      - 您的用户名和密码。

      如果启用了代理并且需要身份验证，则可能需要重新输入用户名和密码。
   b. 单击保存。
4. 重新启动应用程序。

配置 Synopsys Detect 设置

（可选）选择 Synposys Detect，如有必要，定义任何 Synopsys Detect 设置，清除任何不想使用的构建工具，或手动配置构建工具的路径。

检查更新

您可以通过选择更新选项卡来检查 Synopsys Detect (Desktop) 是否有更新。该页面列出了您上次检查更新的时间。单击检查更新以查看是否有可用的较新版本。此选项仅适用于 Windows 和 MacOS 系统。

证书

连接到 Black Duck 时，可以忽略无效或不安全的 SSL 证书。

1. 单击右上角的 将显示“设置”页面。
2. 选择服务器配置选项卡。
3. 选中忽略无效或不安全的 SSL 证书复选框。
4. 重新启动应用程序。

警告：这是一项潜在的不安全操作。只有当您必须连接到具有不安全或自签名证书的系统时，才应使用此操作。

或者，如果要导入自签名证书，可以按照 JRE 的标准 keytool 导入过程执行此操作。

确定 Synopsys Detect 使用的 JRE 的位置：

1. 单击所需组件版本行末尾的 将显示“设置”页面。
2. 选择 Synopsys Detect 选项卡。
3. 从“属性”菜单中选择路径。或者，在搜索属性搜索字段中键入路径以缩小显示的选项范围。
4. 如果 Java 可执行文件字段没有值，Synopsys Detect 将使用在系统环境变量中设置的 $JAVA_HOME 下安装的 JRE。

由于 Synopsys Detect 使用的 JRE 的位置是已知的，应将证书导入到相关 cacerts 文件（通常位于 lib\security 文件夹中）。

1. 在终端会话中，运行以下命令（更改相应的路径）：

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

2. 系统将提示您输入密码。提供密码并按 Enter 键。
3. 系统将提示您是否信任该证书。检查内容并根据需要接受。

注：可能还需要导入与链关联的任何中间证书。如果您在导入过程中遇到任何问题，请联系您的 IT 部门。

扫描选项

Synopsys Detect (Desktop) 使扫描更容易：

- 源目录
- 二进制文件或可执行文件
- Docker 映像或发行版

默认情况下，所有扫描都上传到 Black Duck 服务器并映射到项目版本。但是，您可以按此处所述创建扫描文件，将扫描输出到一个文件，稍后可以将文件上传到 Black Duck。

要指定项目和/或版本名称：

1. 单击项目设置旁边的添加。
2. 选择项目名称和/或版本名称。这些字段将显示在 UI 中。

3. 指定字段的值。

扫描源目录

要扫描源目录：

1. 单击新扫描。
2. 从扫描类型列表中，选择源目录，
3. 单击 以选择要扫描的目录。
4. （可选）通过单击添加并选择设置来修改或配置任何项目或扫描设置。

   如果您购买了代码段扫描许可证并希望启用代码段扫描，请从扫描设置选项中选择代码段匹配并启用它。
5. 单击扫描。

   将显示扫描状态，同时还会显示取消扫描的选项。
6. 扫描完成后，选择本地扫描历史记录选项卡以查看已完成的扫描的信息。从此选项卡中，您可以管理扫描。您也可以使用扫描选项卡查看上传的扫描。

扫描二进制文件/可执行文件

要扫描单个二进制文件或可执行文件：

1. 单击新扫描。
2. 从扫描类型列表中，选择二进制文件/可执行文件，
3. 单击 以选择要扫描的二进制文件或可执行文件。
4. （可选）通过单击添加并选择设置来修改或配置任何项目设置。
5. 单击扫描。

   将显示扫描状态，同时还会显示取消扫描的选项。
6. 扫描完成后，选择本地扫描历史记录选项卡以查看已完成的扫描的信息。从此选项卡中，您可以管理扫描。您也可以使用扫描选项卡查看上传的扫描。

扫描 Docker 映像或发行版

要扫描 Docker 映像或发行版（.tar 文件）：

1. 单击新扫描。
2. 从扫描类型列表中，选择 Docker，
3. 执行以下操作之一：
   - 输入 Docker 映像名称。
   - 选择 选择 Docker 存档 (.tar)，然后单击 以选择要扫描的目录。
4. （可选）通过单击添加并选择设置来修改或配置任何项目设置。
5. 单击扫描。

   将显示扫描状态，同时还会显示取消扫描的选项。
6. 扫描完成后，选择本地扫描历史记录选项卡以查看已完成的扫描的信息。从此选项卡中，您可以管理扫描。您也可以使用扫描选项卡查看上传的扫描。

创建扫描文件

您可以使用 Synopsys Detect (Desktop) 将扫描输出到一个文件中，稍后可以使用 Synopsys Detect (Desktop) 命令行（如下所述）或使用 Black Duck UI 将文件上传到 Black Duck。

注：代码段扫描无法脱机完成，因为它需要与 Black Duck 服务器进行通信。

要创建扫描文件：

1. 单击新扫描。
2. 选择扫描类型（源目录、二进制文件/可执行文件或 Docker）。
3. （可选）通过单击添加并选择设置来修改或配置任何项目或扫描设置（对于源目录扫描）。
4. 选择脱机模式。
5. 单击扫描。

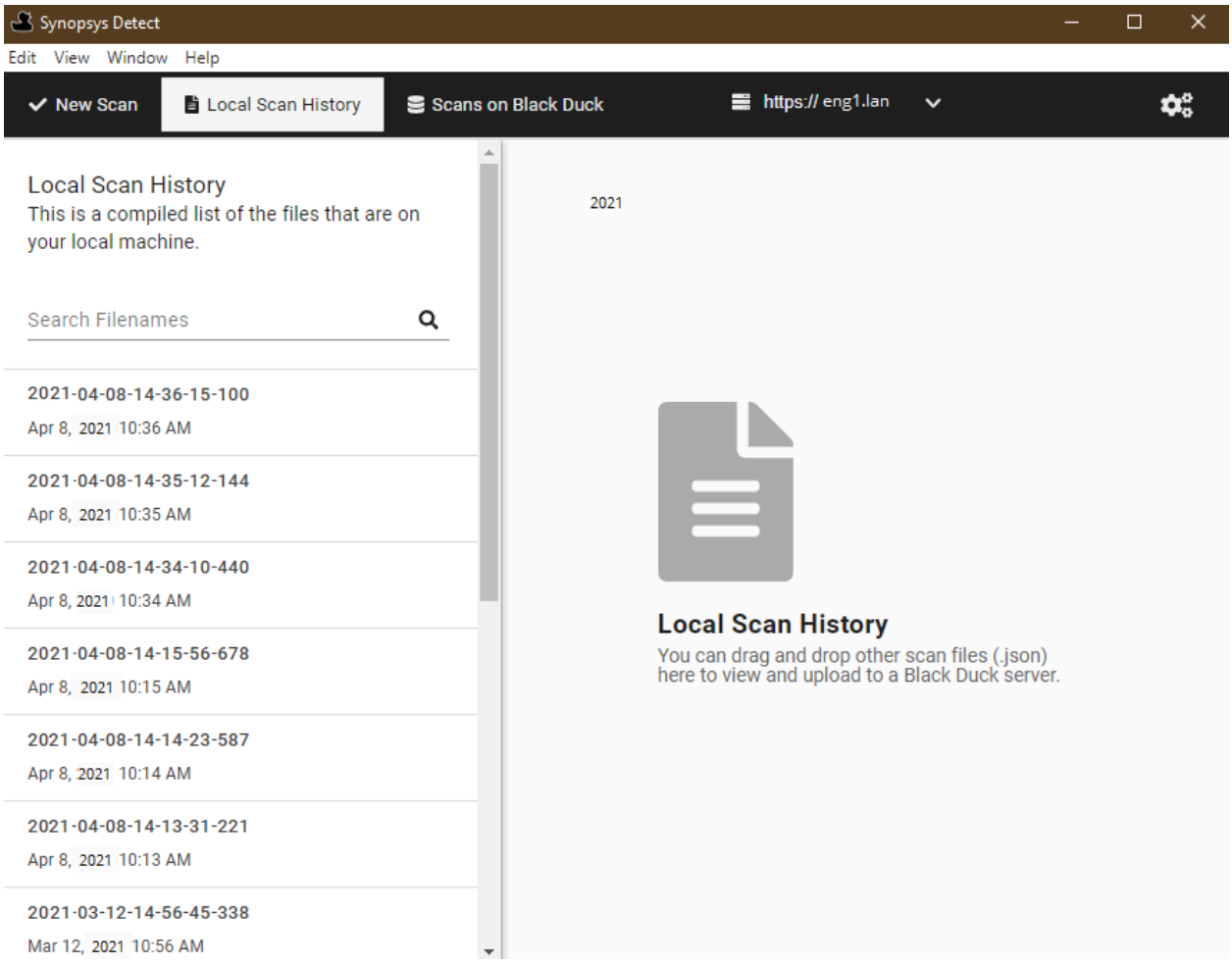
   将显示扫描状态，同时还会显示取消扫描的选项。
6. 扫描完成后，选择本地扫描历史记录选项卡以查看已完成的扫描的信息。

管理扫描

使用本地扫描历史记录选项卡管理扫描。

1. 单击本地扫描历史记录。

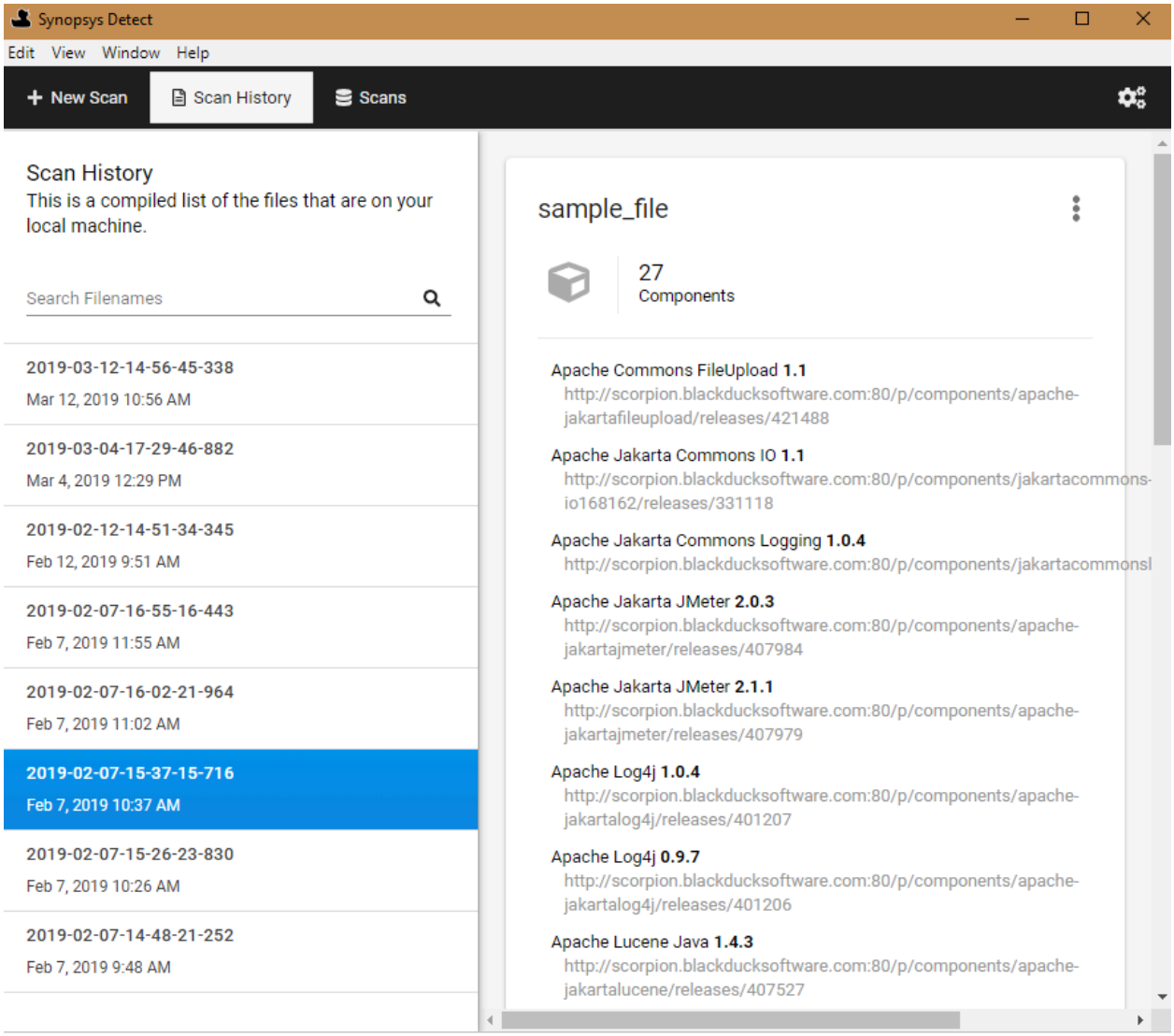
   本地系统上的扫描列表将显示在选项卡的左列中。



   将扫描从本地计算机拖放到此选项卡以进行管理。

   在此选项卡中，选择一个扫描，然后：

   - 查看有关扫描内容的信息：

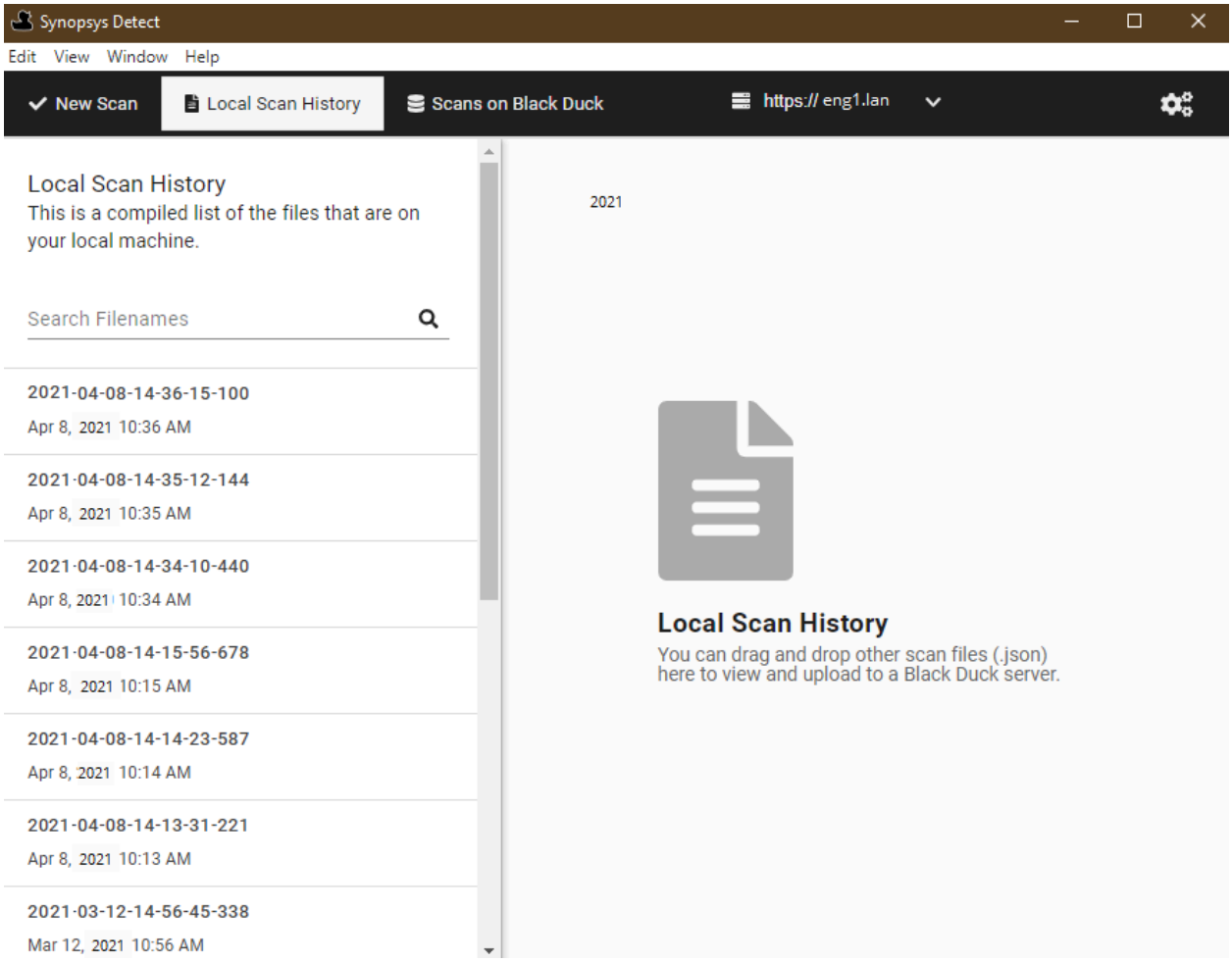


- 通过单击 并选择显示文件来查看文件在系统上的位置。
- 上传文件，如下一节所述。
- 将鼠标悬停在左列中的扫描名称上，然后单击删除以删除扫描。单击是进行确认。

将扫描文件上传到 Black Duck

您可以使用 Synopsys Detect (Desktop) 将扫描文件上传到 Black Duck。

1. 单击本地扫描历史记录。

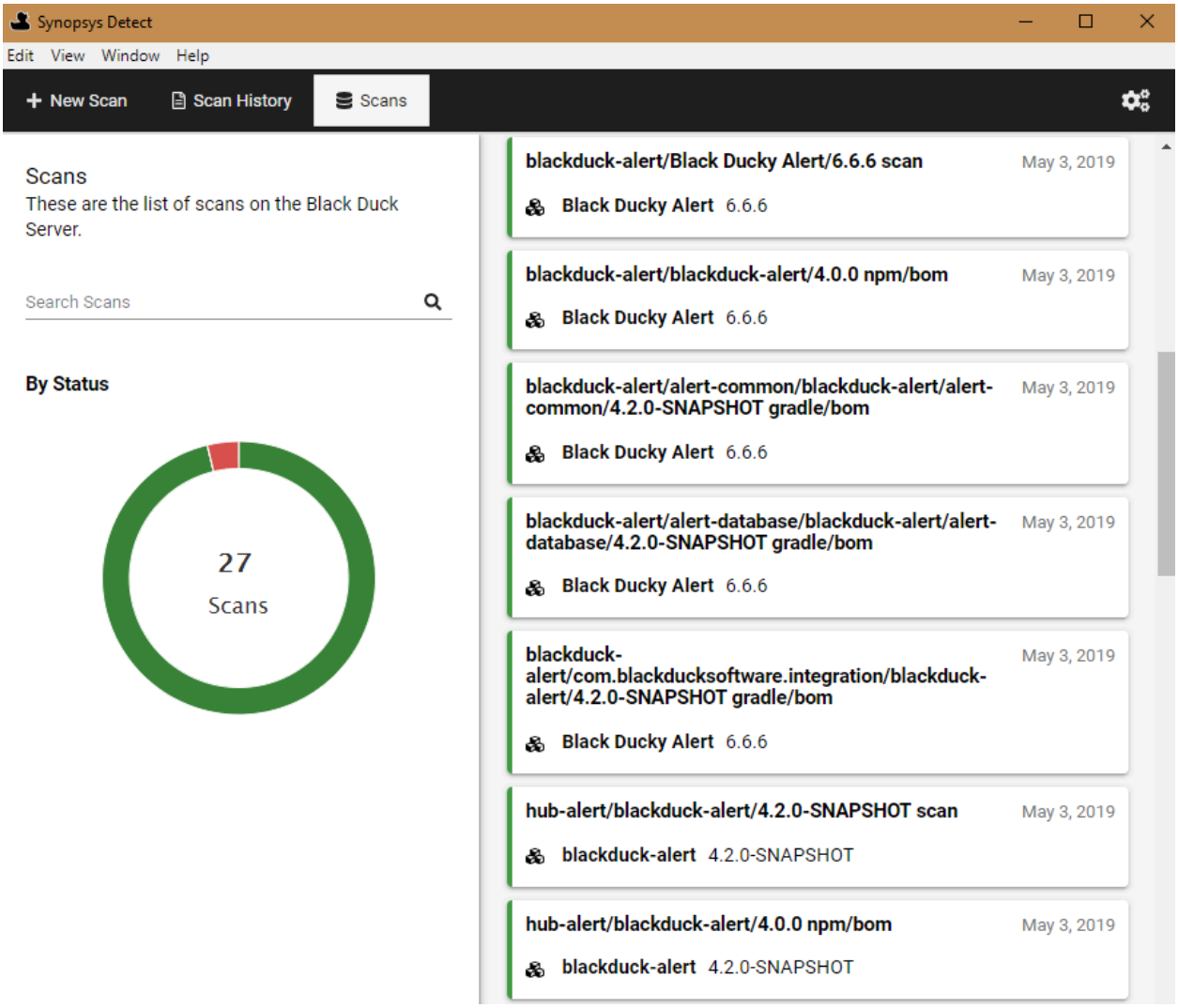


2. 如果文件位于本地系统上，则可以将扫描文件从本地计算机拖放到扫描历史记录选项卡。
3. 选择要上传的文件，然后单击右上角的 ⋮ 以显示文件选项。
4. 单击将扫描文件上传到 Black Duck。将出现“上传进度”窗口，显示上传状态。此过程完成后，关闭窗口。

   您可以通过单击扫描并查看上传的文件来确认扫描已上传。

查看上传的扫描

您可以通过单击 Black Duck 上的扫描来查看已上传到 Black Duck UI 的扫描：



此选项卡显示以下信息：

- 选项卡的左侧按状态（正在进行、已完成或错误）显示已上传的扫描。

  使用搜索字段查找扫描或限制显示的扫描。
- 页面右侧列出了扫描并显示了每个扫描的以下信息：
  - 名称
  - 项目和项目版本扫描映射到项目，或指示扫描未映射到项目。
  - 扫描上传至 Black Duck 的日期。

选择一个扫描以打开 Black Duck 中所选扫描的扫描名称页面。

注：Synopsys Detect (Desktop) 中显示的扫描字节数可能与 Black Duck 中显示的扫描字节数不同。原因在于 Black Duck 计算和统计使用的字节数的方式。这是正常现象，预计在某些扫描中会发生。

创建项目

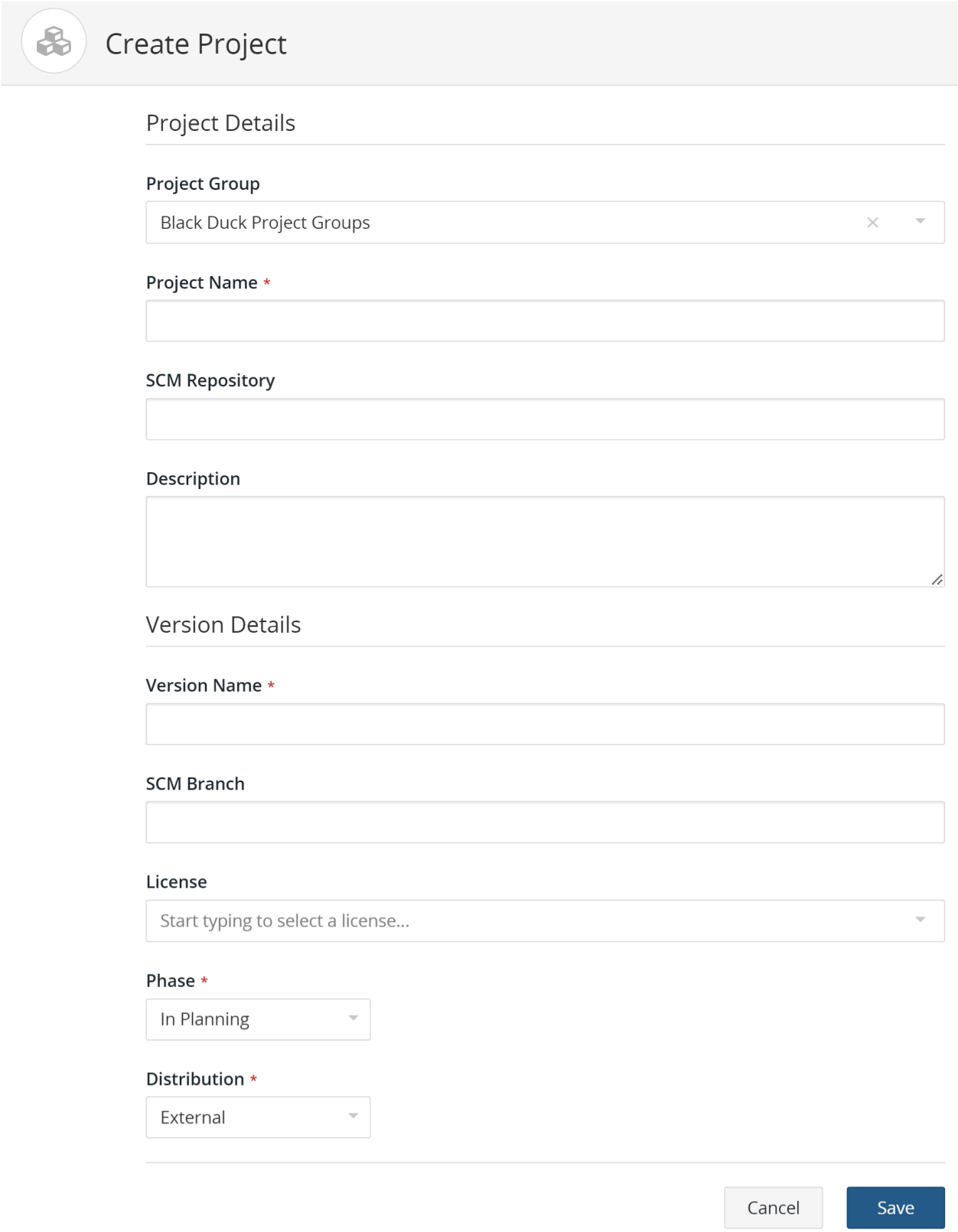
项目是 Black Duck 中的基本单位。项目既可以是一个独立的开发项目，也可以是另一个项目的一部分。例如，Apache Tomcat 本身就是一个项目，但它也可能是其他大型项目的一部分。您必须创建要提供给组织中的其他开发人员搜索的项目。

请注意，项目或应用程序的托管代码库限制为 10GB。

要创建项目：

1. 登录 Black Duck。

2. 单击任意页面顶部的 + 创建项目。此时将显示项目详细信息页面。



3. 输入项目名称。此名称在 Black Duck 中的项目间必须是唯一的，但是，它可以与 Black Duck KB 中的项目具有相同的名称。

   提示：作为最佳做法，在创建项目名称时，您应该考虑其他用户会如何搜索您的项目。例如，如果您的项目与 3D 图形相关，将其命名为“3DGraphics”意味着，用户必须键入整个项目名称才能找到您的项目。如果您在名称中使用空格或下划线，例如“3D Graphics”或“3D_Graphics”，则附加的分隔符将允许用户使用搜索词“3D”查找项目。

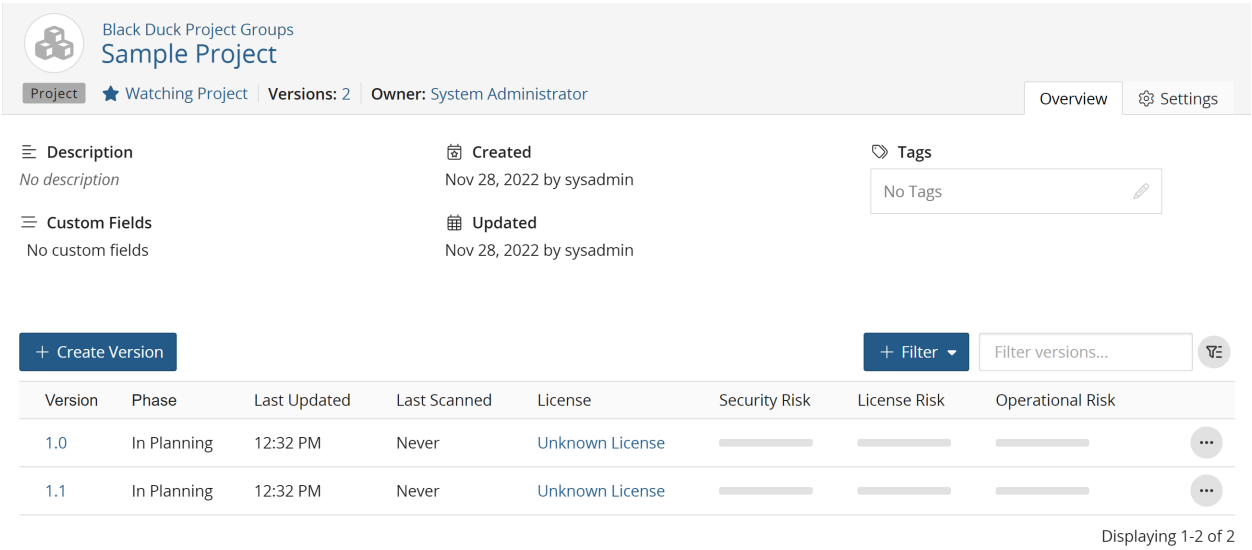
4. （可选）输入其他信息，例如：

   - SCM 存储库：代码所在的源代码管理 (SCM) 存储库的 URL。只有在您的环境中启用了此功能时，此字段才可见。完成软件包管理器扫描后，可以手动编辑或通过 Detect 自动填充。如果 URL 不匹配，手动更改 SCM 存储库 URL 可能会中断现有扫描。请注意，此功能仅适用于 Detect 8.x。
   - 说明：作为最佳做法，在创建项目说明时，您应该考虑其他用户会如何搜索您的项目。说明应具体描述项目的用途及其独特性，以便与其他类似项目轻松区分。

5. 在版本名称字段中键入此项目的版本。

6. 默认情况下，对该项目的某个版本所做的编辑将应用于该项目的所有版本，不包括存档版本和手动添加的组件。如果您希望编辑仅应用于特定版本，请清除此选项。

7. 单击保存。
   Black Duck 显示项目名称页面。



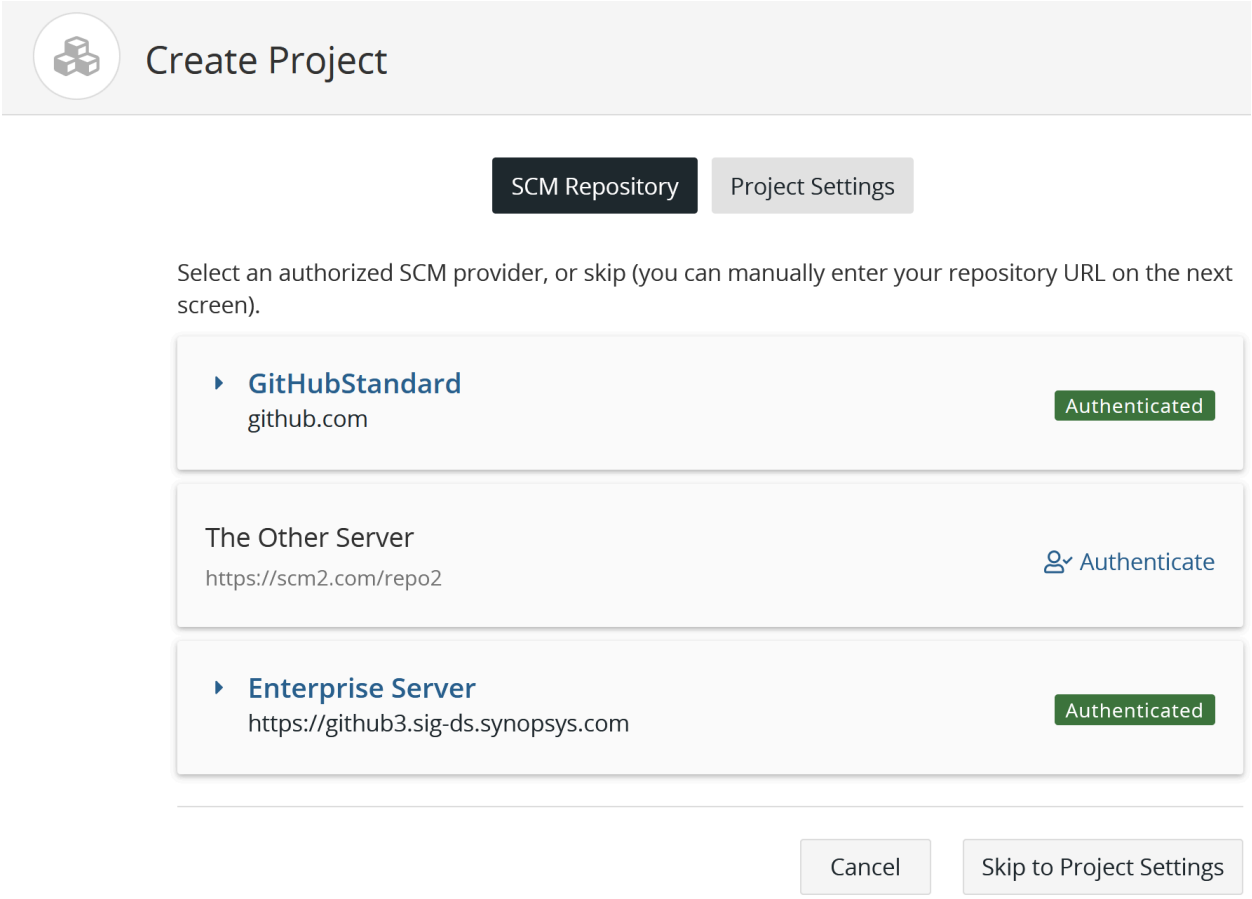
创建启用了 SCM 集成的项目

如果启用了 SCM 集成，则创建项目的过程会添加一个额外的步骤，以选择项目来源的 SCM 存储库。显示的服务器将取决于您的组织已配置使用的 SCM 提供商。

要创建项目：

1. 登录 Black Duck。
2. 单击任意页面顶部的 + 创建项目。

3. 从显示的选项中选择授权的 SCM 提供商。



4. 选择适用于您的项目的 SCM 提供商。您必须经过身份验证才能使用 SCM 提供商。
5. 从 SCM 存储库下拉菜单中选择存储库。
6. 从 SCM 分支下拉菜单中选择分支。
7. 单击选择。然后，您将转到项目设置页面，该页面遵循上述详细流程。“SCM 存储库”和“SCM 分支”字段将使用先前选择的选项自动填充。

将扫描映射到项目

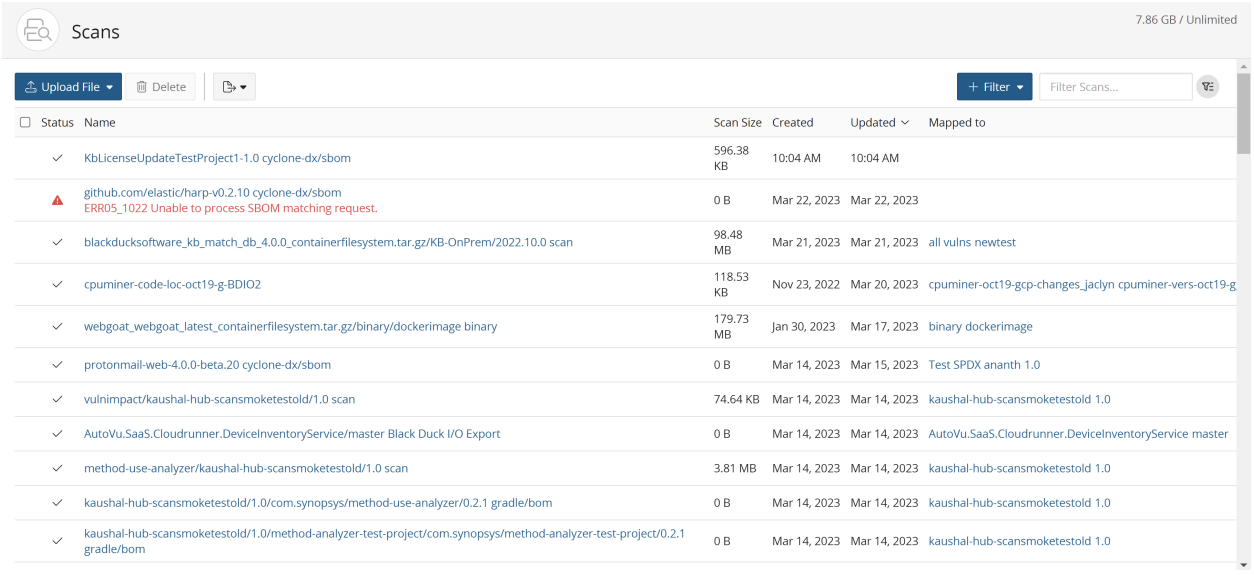
映射扫描会将扫描数据添加到项目版本的 BOM。

注：您可以多次扫描 Docker 映像或文件目录位置或存档，但只需将其映射到项目版本一次。主机和路径可能会更改，但只要代码位置名称相同，Black Duck 就会使用后续扫描期间发现的任何新信息自动更新项目的 BOM。

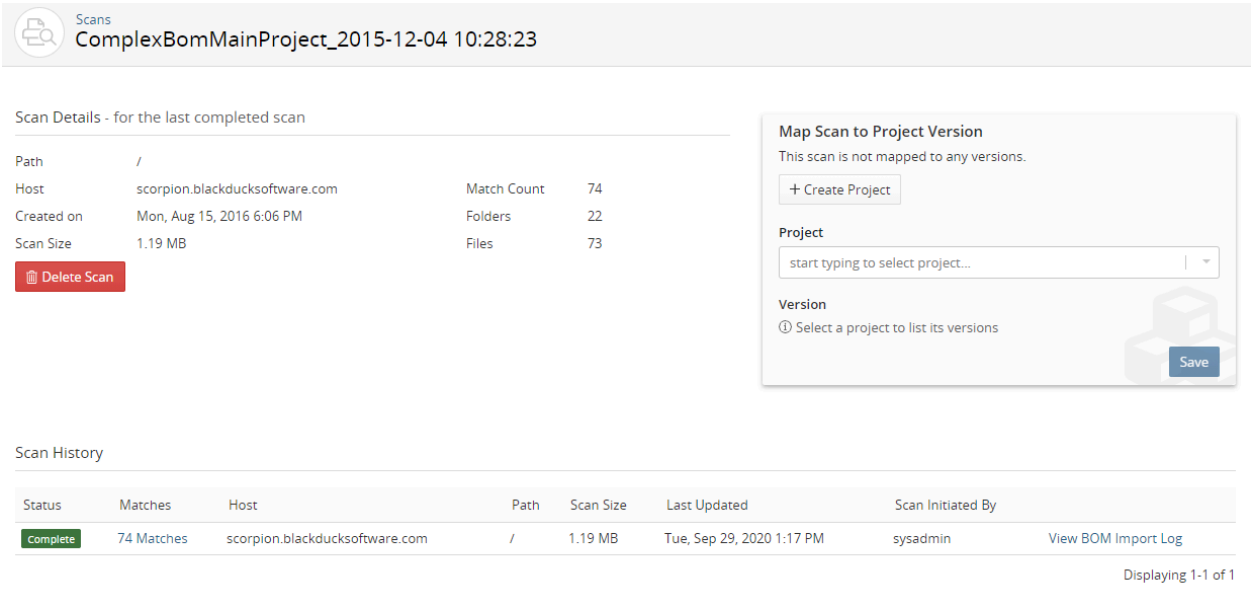
要将扫描映射到项目：

1. 登录 Black Duck。

2. 单击 Scans。



3. 执行以下操作之一：
   - 单击 ，并选择映射到项目。
   - 选择要映射的扫描路径以打开扫描名称页面。



4. 开始键入项目的名称，以便在项目字段中渐进显示匹配项。
   如有必要，选择创建项目以创建新项目和版本。
5. 选择要将组件扫描映射到的项目版本。
   如有必要，选择创建版本以为项目创建新版本。

6. 单击保存。
   Black Duck 显示将组件扫描映射到的项目的名称和版本。选择链接以打开 BOM 页面。

   注: Black Duck 显示聚合项目版本 BOM。如果组件版本在存档中出现多次，则只在 BOM 中显示一次。

4. 查看 中的风险 Black Duck

Black Duck 帮助您在多个详细级别了解项目中的风险类型和严重性。用于计算风险的数据由 Black Duck KB 提供。

使用以下页面识别和管理项目中的风险：

- “仪表板”页面
- 项目版本页面/组件选项卡
- 项目版本页面/安全选项卡

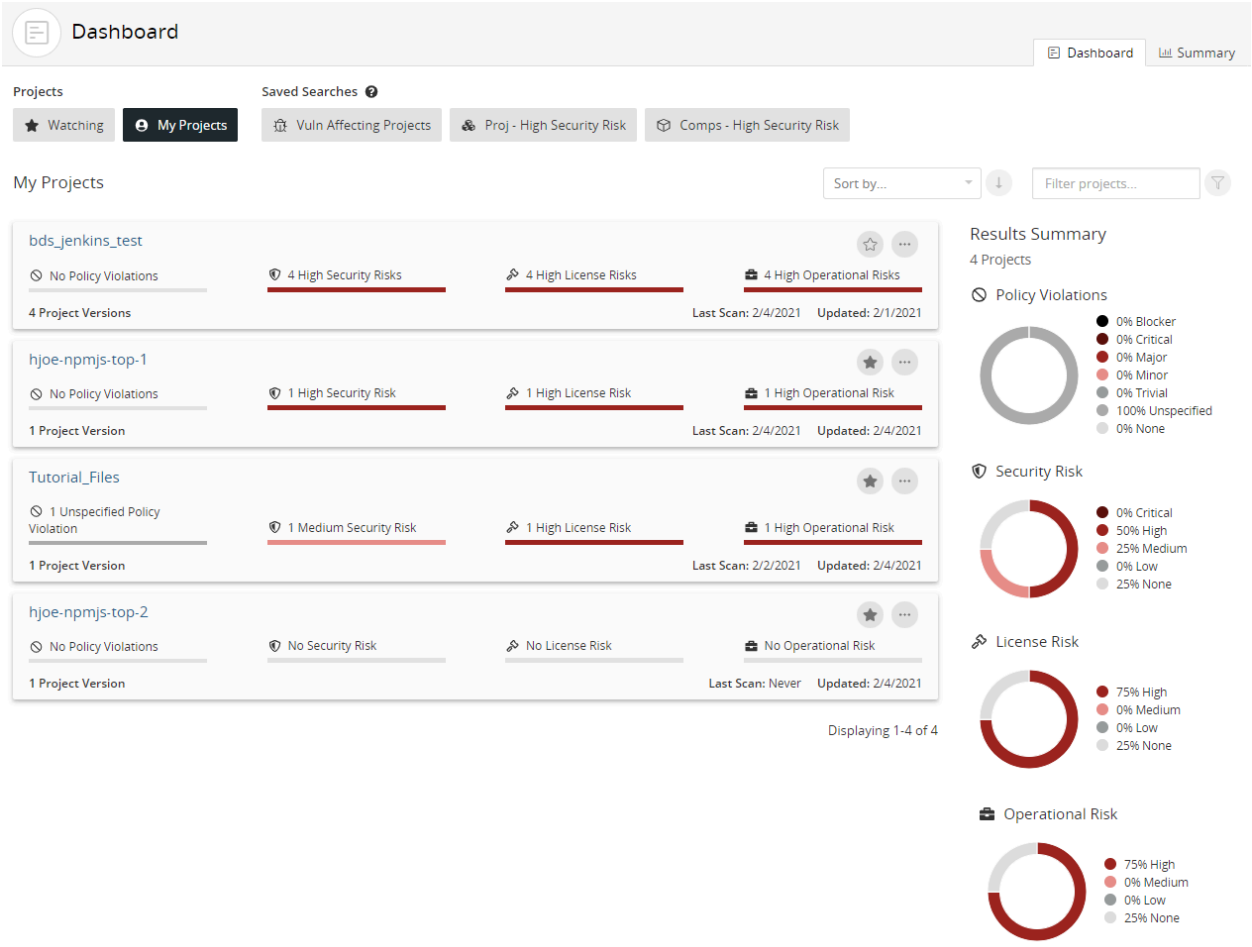
请注意，显示的安全风险值使用 CVSS v2 或 CVSS v3.x 分数，具体取决于您选择的安全风险计算；默认情况下，将显示 CVSS v3.x分数。请注意，如果您选择了 CVSS v2，安全风险图形将显示值为 0 的“严重”风险类别。

仪表板

仪表板从不同角度提供了风险的高级概述。

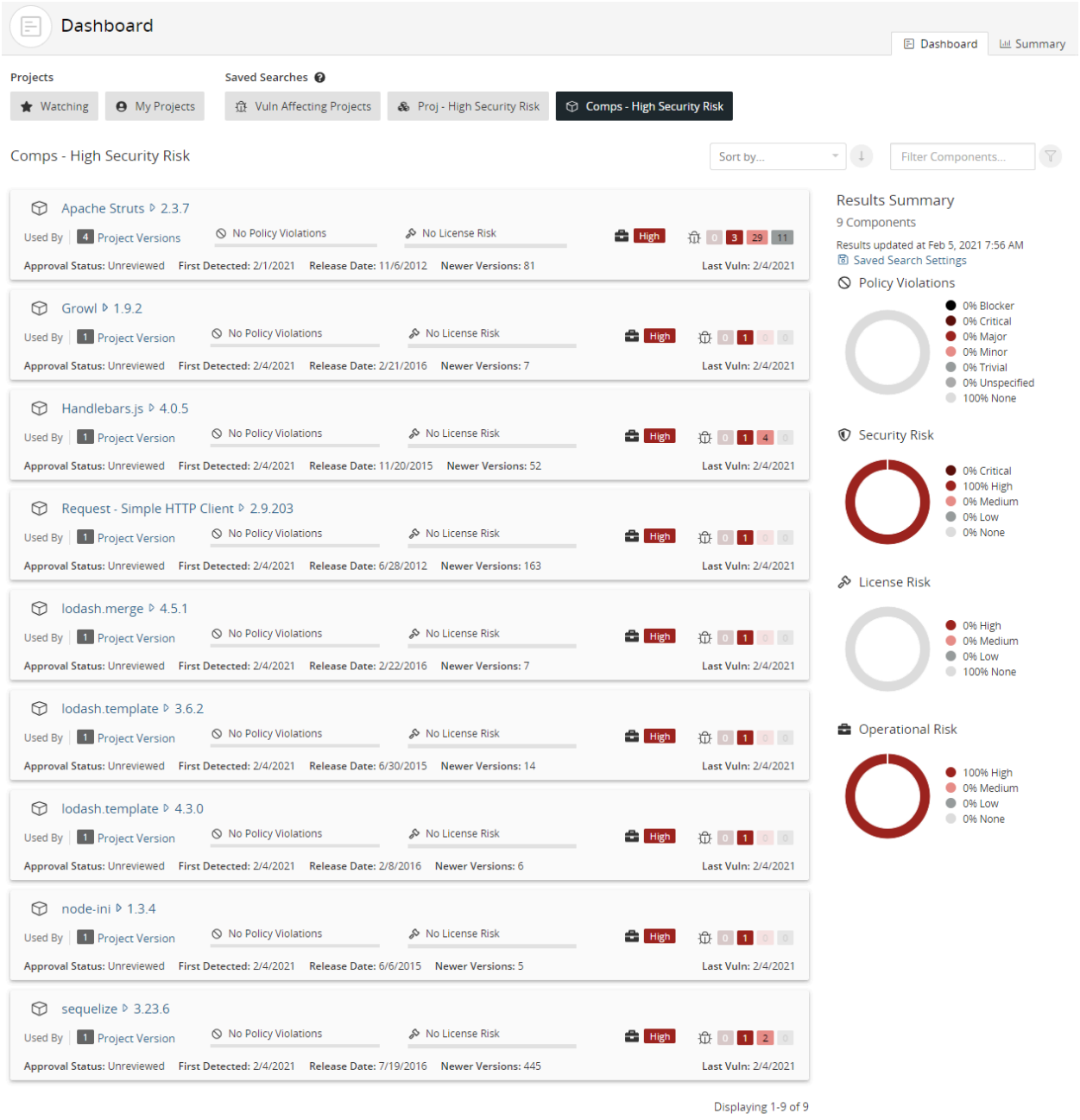
注：在您创建项目并将扫描映射到这些项目或手动将组件添加到 BOM 之前，仪表板不会包含任何项目或组件信息。然后，项目版本 BOM 中组件的风险信息将显示在“仪表板”页面上。

- 您可以使用正在关注或我的项目仪表板查看感兴趣的项目，也可以通过保存项目搜索结果来创建自定义仪表板。

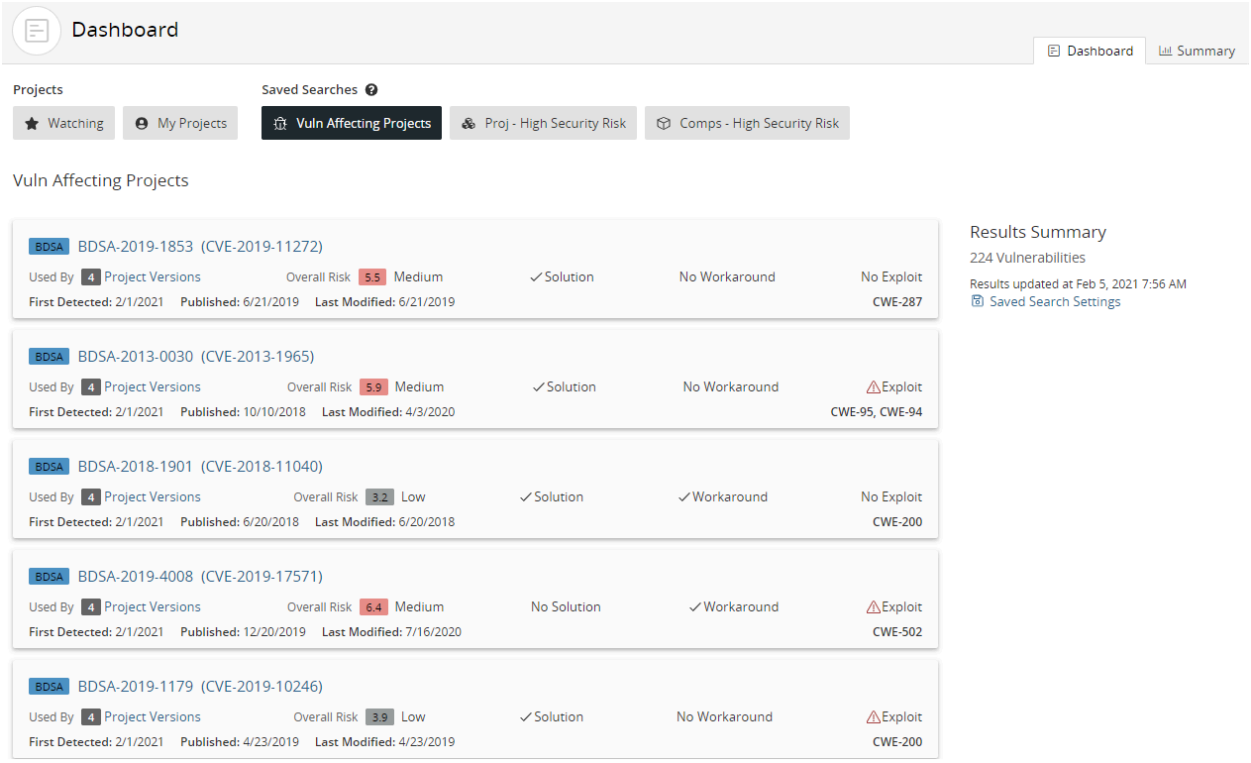


创建保存的组件搜索以查看您感兴趣的在一个或多个项目中使用的组件。

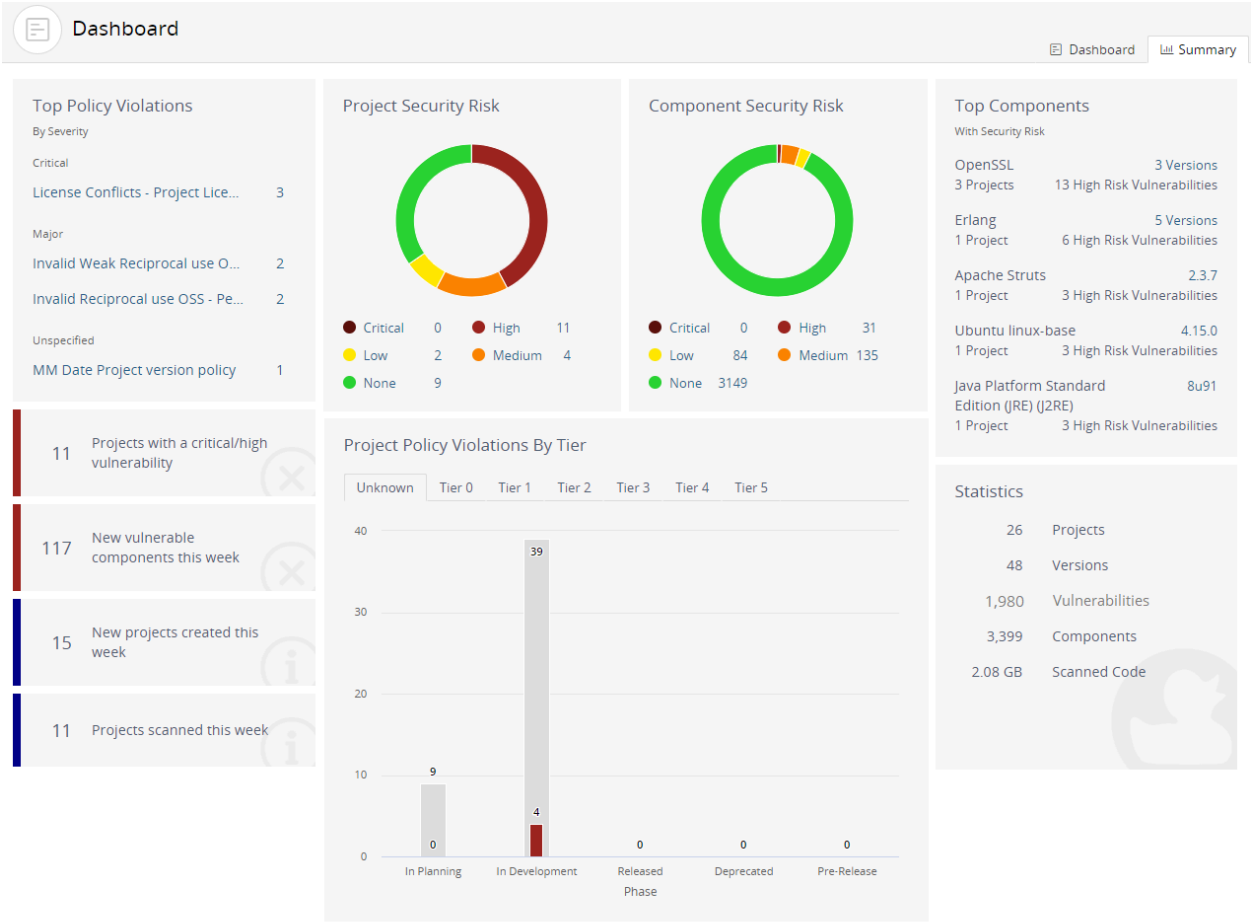
4. 查看 中的风险 Black Duck • 仪表板



- 创建保存的漏洞搜索以查看您感兴趣的漏洞。



- 使用摘要仪表板查看您有权查看的项目的整体运行状况并确定关注领域。

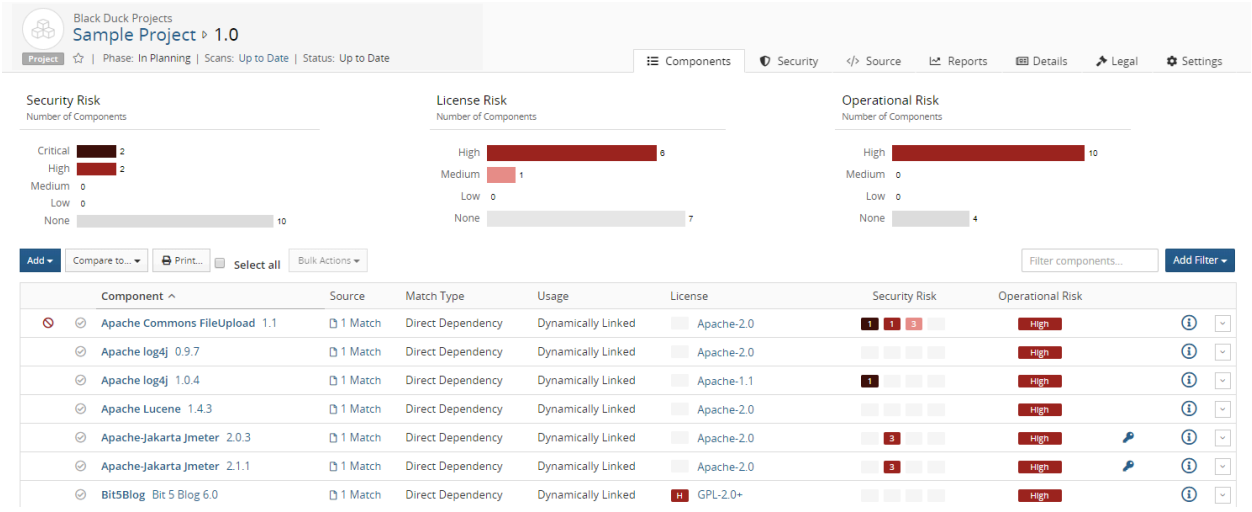


注:

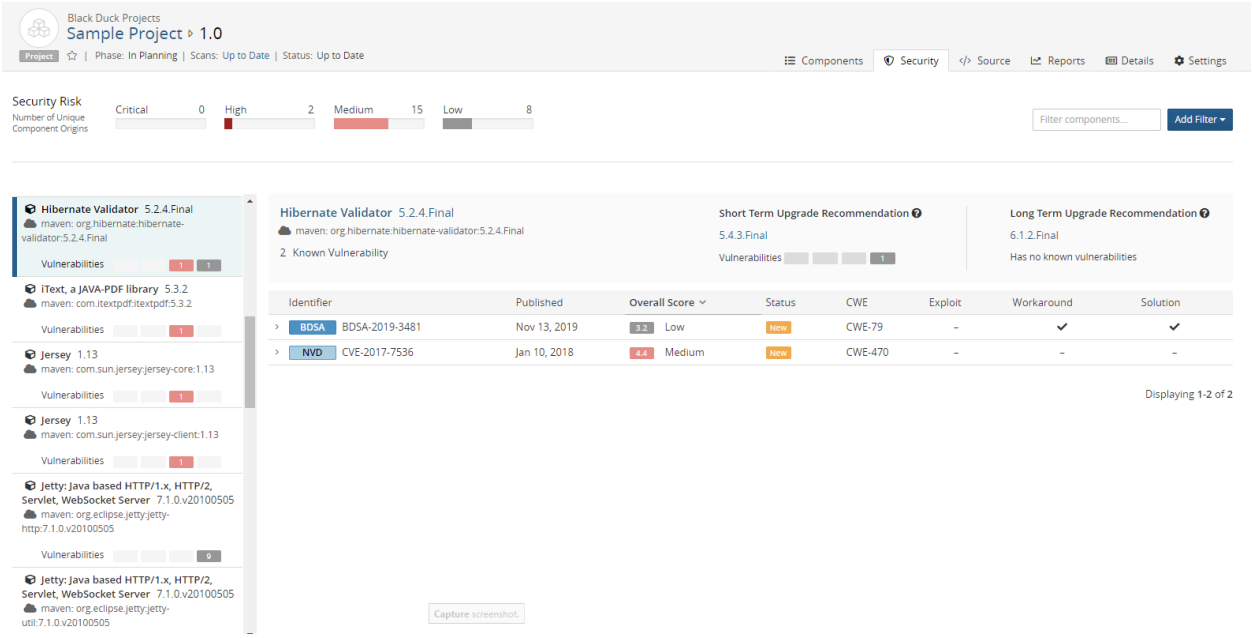
- 登录时显示的“仪表板”页面取决于您在先前注销之前查看的最后一个主仪表板（“仪表板”或“摘要”）。
- 单击 Dashboard 或导航栏左上角的徽标以查看您查看的最后一个仪表板（“仪表板”或“摘要”）。

项目版本页面

- 使用项目版本页面/组件选项卡（也称为项目版本 BOM），以查看特定于该项目版本且具有安全风险、许可证风险和操作风险的组件。



- 使用项目版本页面/安全选项卡，以查看与项目版本中使用的组件相关的每个严重性的安全漏洞。



查看仪表板

使用仪表板查看与一个或多个项目版本中的组件相关的风险和策略违反的类型和严重程度。仪表板提供了项目、组件和漏洞的整体视图。

为了让您能够查看对您至关重要的项目和项目版本，Black Duck 提供了两个默认仪表板，并且您可以创建数量不限的自定义仪表板。

Black Duck 显示以下两个默认仪表板：

- 正在关注。您关注的项目。
- 我的项目。您的所有项目，包括您没有关注的项目。

这些仪表板在项目级别的“仪表板”页面上显示信息。

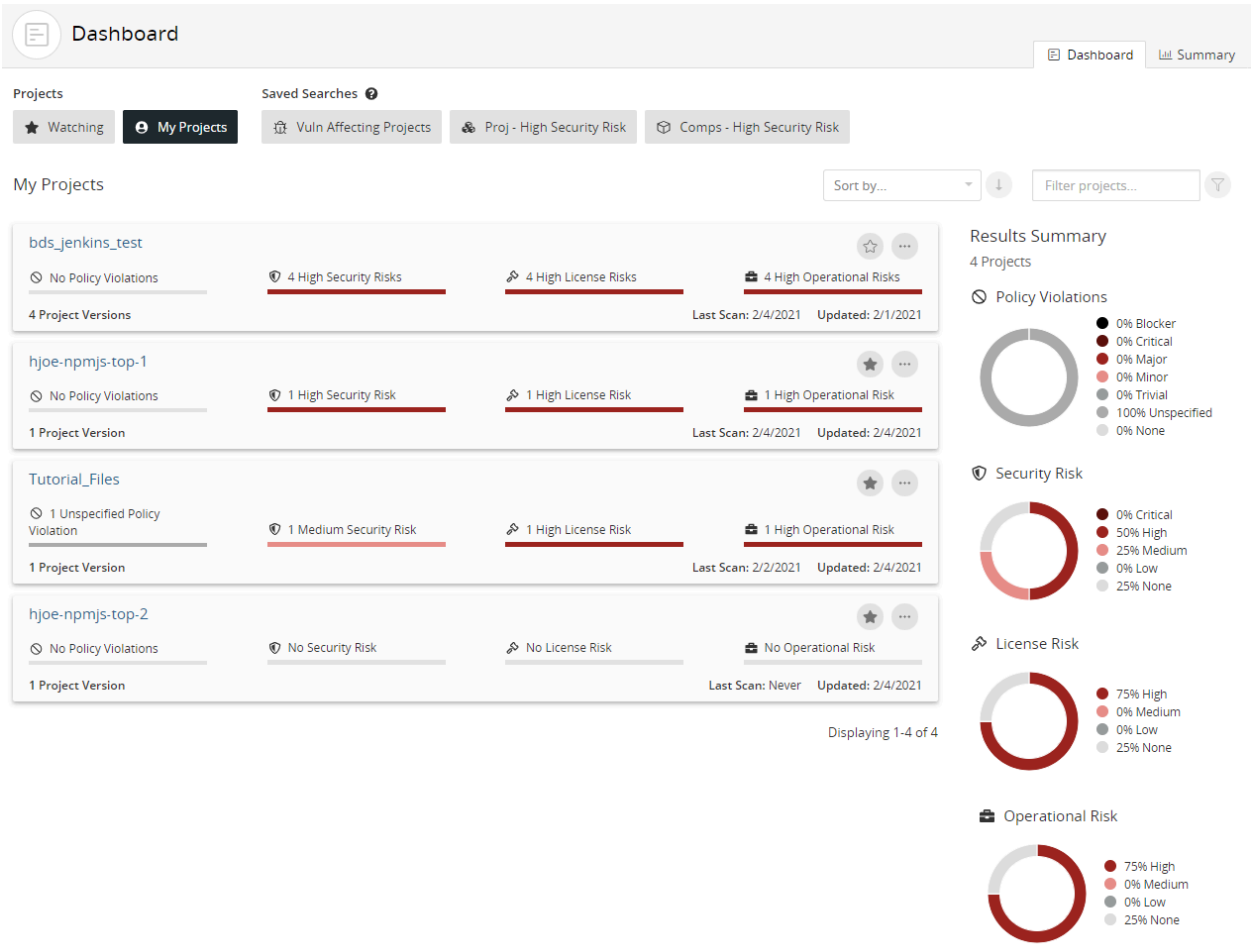
此外，您还可以创建自定义仪表板，以便快速查看对您至关重要的项目版本、组件版本和漏洞：搜索项目、组件和/或漏洞，然后保存搜索；使用“仪表板”页面查看这些已保存搜索的信息。

查看仪表板

要查看仪表板：

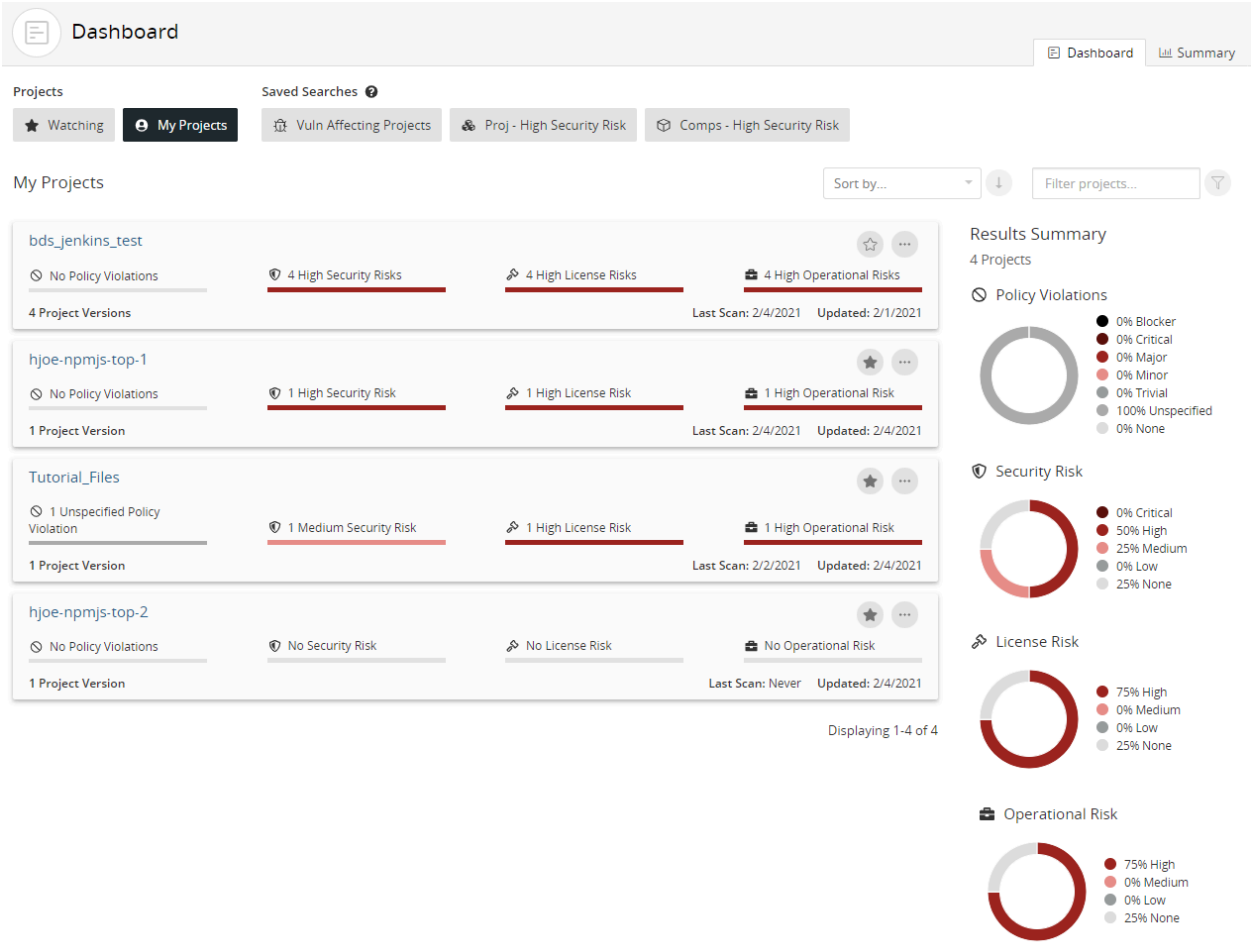
1. 单击 Dashboard 以显示仪表板。

   显示的仪表板页面取决于您之前查看的最后一个仪表板（特定仪表板页面或摘要仪表板）。如果未显示，请选择仪表板以显示仪表板。

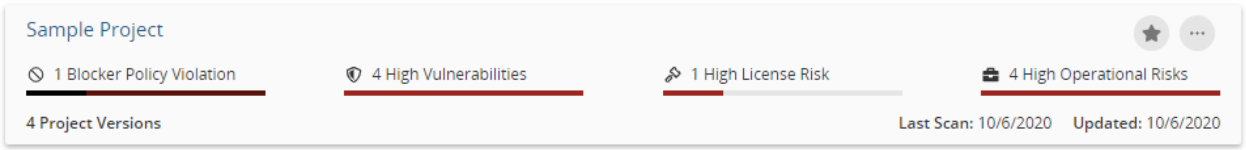


关于“正在关注”和“我的项目”仪表板

使用正在关注或我的项目仪表板查看项目级别的风险和策略违反信息。

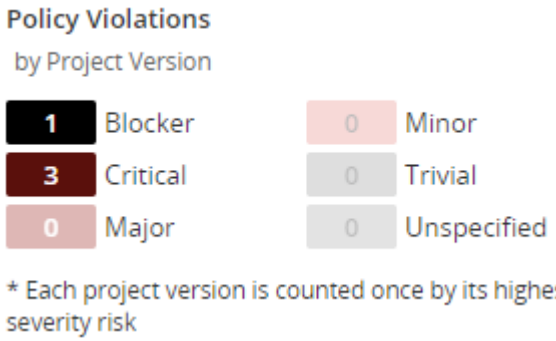


为每个项目显示以下信息：



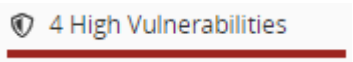
- 要查看特定项目的策略违反信息：
  - 使用条形图查看策略严重性级别最高的项目版本的数量。

    注：文本说明了具有此最高策略严重性级别的项目版本数，而不是影响此项目的所有策略严重性级别。
  - 将鼠标悬停在条形图上可查看具有最高严重性级别的策略违反的项目版本数：

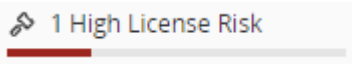
    

    在上面的示例中，有四个项目版本存在策略违反；一个版本的策略违反将“阻止”作为最高严重性级别，而其他三个版本则将“严重”定为最高严重性级别。请注意，这并不表示这些版本中的策略违反数量，只表示每个版本的最高严重性级别。
- 要查看风险信息：
  - 使用条形图查看风险级别最高的项目版本的数量：

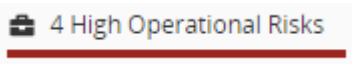
    安全风险：

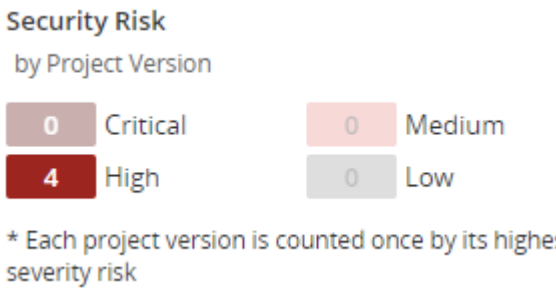
    许可证风险：

    操作风险：

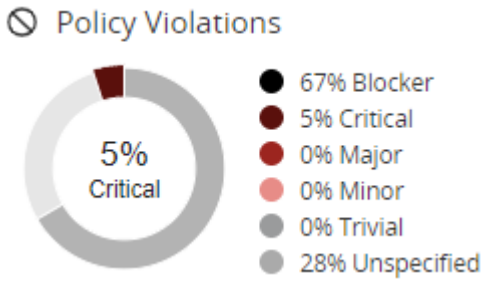
    

    注：文本说明了具有此最高风险级别的项目版本的数量，而不是影响版本的所有风险级别。
  - 将鼠标悬停在风险条形图上可查看此项目具有最高风险级别的版本数。

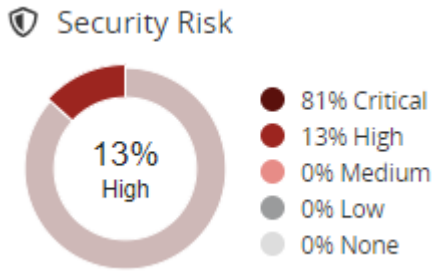
    

    如果项目版本有风险，则只对该版本进行一次计数，并且只显示其最高风险级别。

- 使用图形查看此仪表板中所有项目的概览信息。
  - 风险图形按严重性级别显示此仪表板中具有策略违反的项目的百分比。您也可以将鼠标悬停在图形中的某个区域上以查看此信息：



  - 风险图形显示此仪表板中具有此安全风险、许可证风险或操作风险级别的项目的百分比。您也可以将鼠标悬停在图形中的某个区域上以查看此信息：

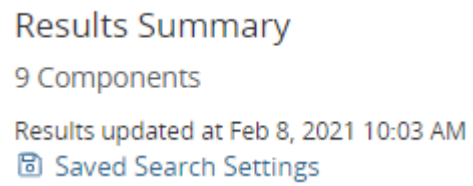


  - 将鼠标悬停在图例中的值上以突出显示图形中的值。
- 查看每个项目的其他信息，包括：
  - 版本数。
  - 上次扫描日期。
  - 上次更新此项目的日期，例如上次运行映射到任何项目版本的扫描的时间，或上次更新任何项目版本的 BOM 的时间（手动或通过新扫描）。
- 选择项目名称以查看列出此项目所有版本的项目名称页面。
- 管理项目在这些仪表板中的显示方式：
  - 使用排序依据字段选择要排序的属性，然后单击箭头以选择排序顺序 ↑（升序）或 ↓（降序）。
  - 使用过滤项目字段过滤任一仪表板中显示的项目。
- 使用图标 以管理您关注的项目或删除项目。

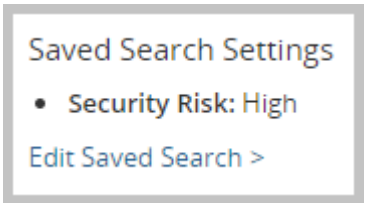
关于保存的搜索仪表板

使用保存的搜索查看对您至关重要的项目版本、组件版本和漏洞。

对于每个已保存的搜索，Black Duck 会列出上次更新此搜索的日期和时间。

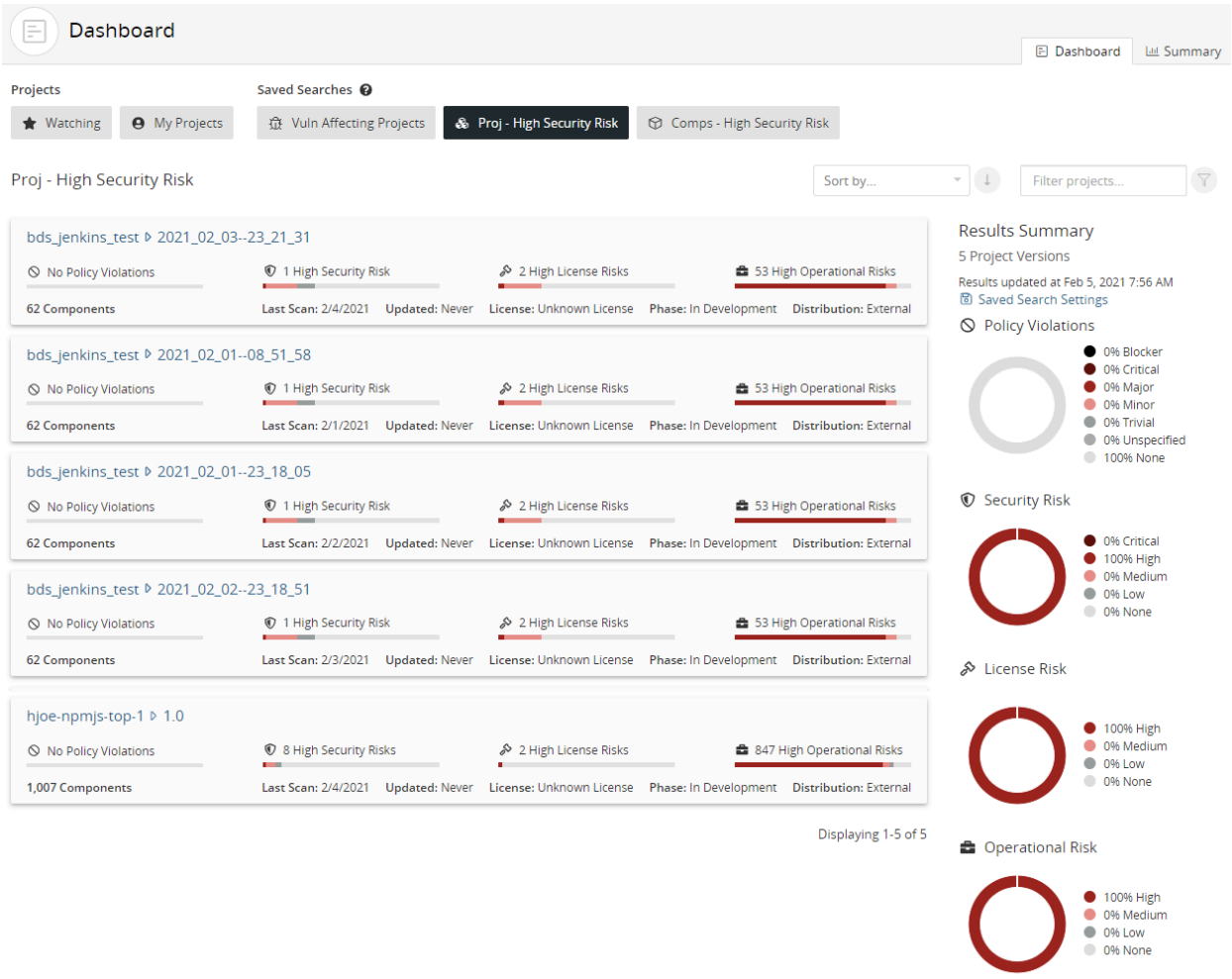


选择已保存的搜索设置以查看此已保存搜索的过滤器。

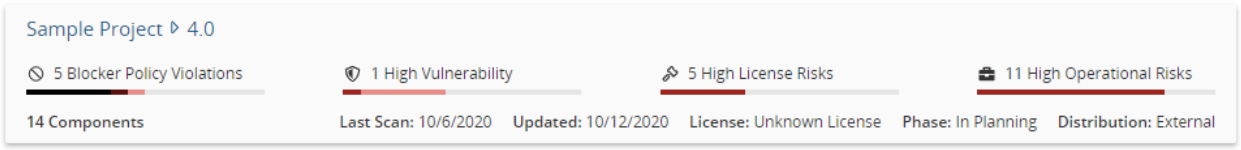


选择编辑保存的搜索以打开显示已保存搜索的“查找”页面。使用页面编辑并保存此修订后的已保存搜索。

项目版本保存的搜索



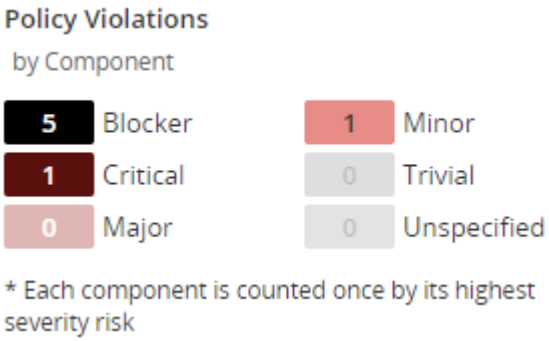
为每个项目版本显示以下信息：



- 位于保存的搜索名称前面表示这是项目保存的搜索。
- 要查看特定项目版本的策略违反信息：
  - 使用条形图查看此项目版本具有该最高策略严重性级别的组件数。

    例如，下面显示，虽然存在严重性级别较低的组件，但此项目版本的最高策略严重性级别为“阻止”，并且有五个组件的最高策略严重性级别是“阻止”。

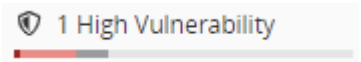
    注：文本说明了此项目版本具有最高策略严重性级别的组件数，而不是影响此项目版本的所有策略严重性级别。
  - 将鼠标悬停在条形图上以查看按最高策略严重性级别列出的已违反策略的组件数：

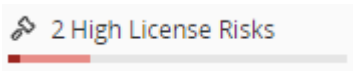
    如果组件存在策略违反，则仅对该组件进行一次计数，并且只显示其最高策略严重性级别。

- 要查看风险信息：
  - 使用风险条形图快速查看安全性风险、许可证风险或操作风险级别最高的组件数量。

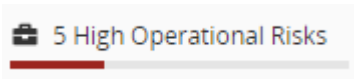
    安全风险：

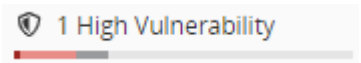
    许可证风险：

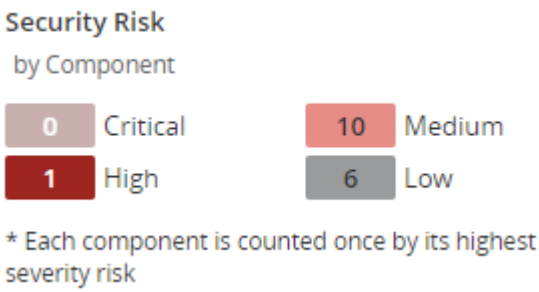
    操作风险：

    例如，下面显示虽然存在风险较低的组件，但此项目版本的安全风险为“高”，并且此项目版本中的一个组件的最高风险级别是高安全风险级别：

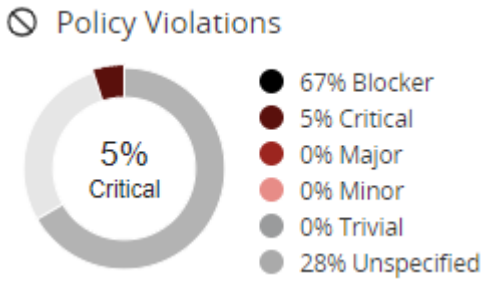
  - 将鼠标悬停在条形图上以查看每个风险类别的组件数量。

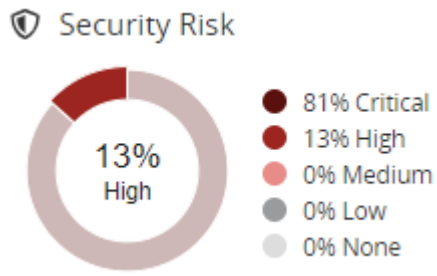
    在此示例中，有一个组件的最高风险级别为高风险，10 个组件的最高风险级别为中等风险，六个组件的最高风险级别为低风险。

    注：每个组件仅计数一次，并且按最高风险级别显示。

- 使用图形查看此仪表板中按策略严重性和风险级别分类的所有项目版本的概述信息。图形列出了每个级别的百分比。您还可以：
  - 将鼠标悬停在图形上，查看每个策略严重性级别存在策略违反的项目版本的百分比。

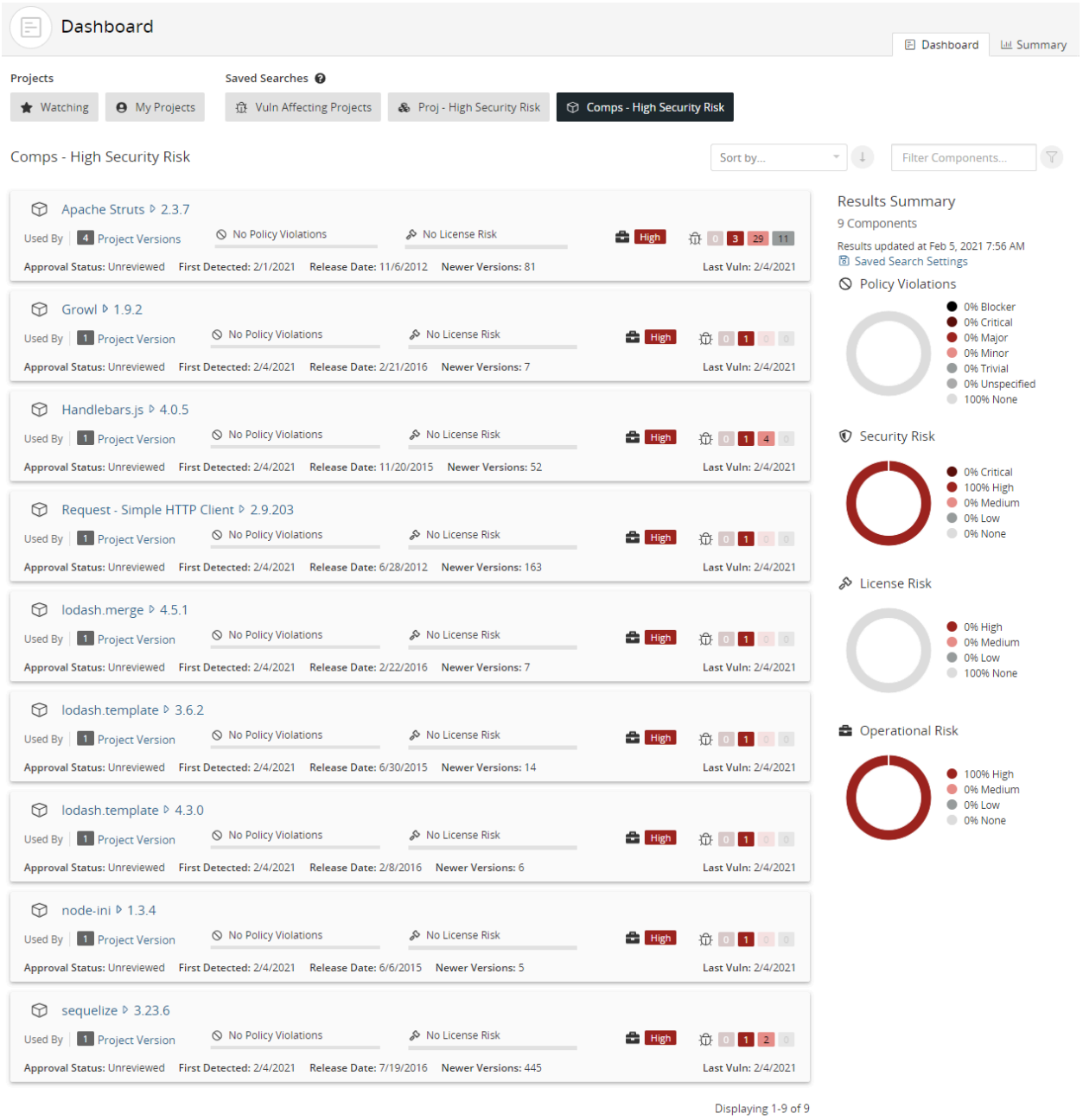


  - 将鼠标悬停在图形上，查看此仪表板中每个风险级别的项目版本百分比。

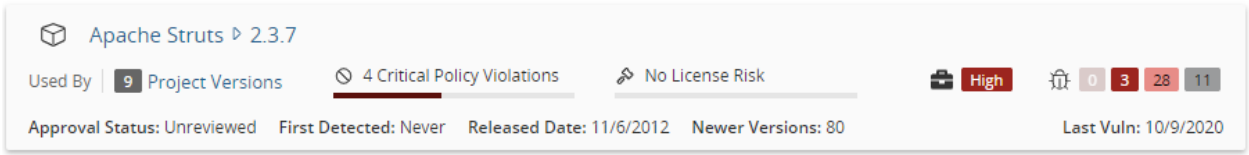


  - 将鼠标悬停在图例中的值上以突出显示图形中的值。
- 对于每个项目版本，仪表板还显示：
  - 此项目版本中的组件数。
  - 上次扫描日期。
  - 上次更新此项目版本的日期，例如上次运行映射到此项目版本的扫描的时间，或上次更新此项目版本的 BOM 的时间（手动或通过新扫描）。
  - 此项目版本的许可证。
  - 此项目版本的阶段。
  - 此项目版本的分发。
- 选择项目或版本名称以查看 BOM。
- 管理项目在这些仪表板中的显示方式：
  - 使用排序依据字段选择要排序的属性，然后单击箭头以选择排序顺序 ↑（升序）或 ↓（降序）。
  - 使用过滤项目字段以过滤仪表板中显示的项目。

组件保存的搜索

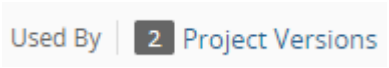


为每个组件显示以下信息。

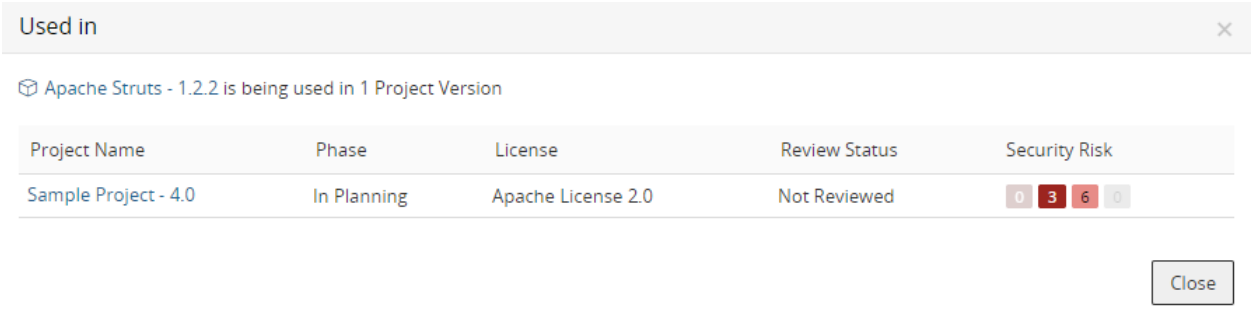


- 位于保存的搜索名称前面表示这是组件保存的搜索。
- 选择组件名称/版本以显示组件名称版本页面。

- 查看使用此组件版本的项目版本数，如使用者旁边的值所示。



选择项目版本以打开“使用位置”对话框。

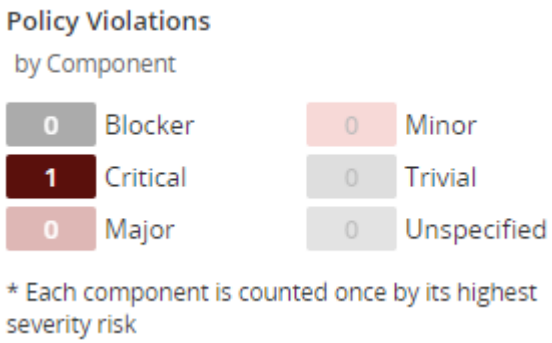


此对话框显示使用此版本组件的项目版本。

列	说明
项目名称	使用此组件版本的项目和版本的名称。选择项目名称以显示项目版本的组件选项卡。
阶段	项目阶段。
许可证	此组件版本的许可证。
审核状态	是否已在此项目版本中审查此组件。
安全风险	从左到右列出每个严重级别的漏洞：严重、高、中和低。 选择一个值以显示 Black Duck KB 组件名称版本页面的安全选项卡，其中列出了与此组件版本关联的漏洞。

- 使用条形图快速查看策略严重性级别最高的组件数量。

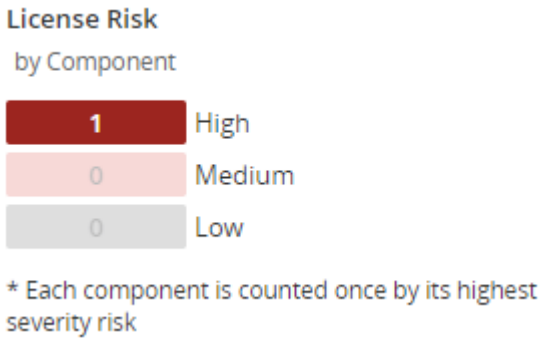
选择条形图以查看按严重性级别列出的已违反策略的组件数：



注：一个组件仅按最高的策略严重性级别计数一次，而不是按影响此组件的所有策略严重性级别进行计数。

- 使用条形图快速查看许可证风险级别最高的组件数量。

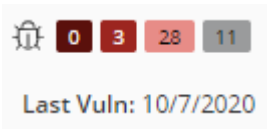
  选择条形图以查看每个风险类别中的组件数量。

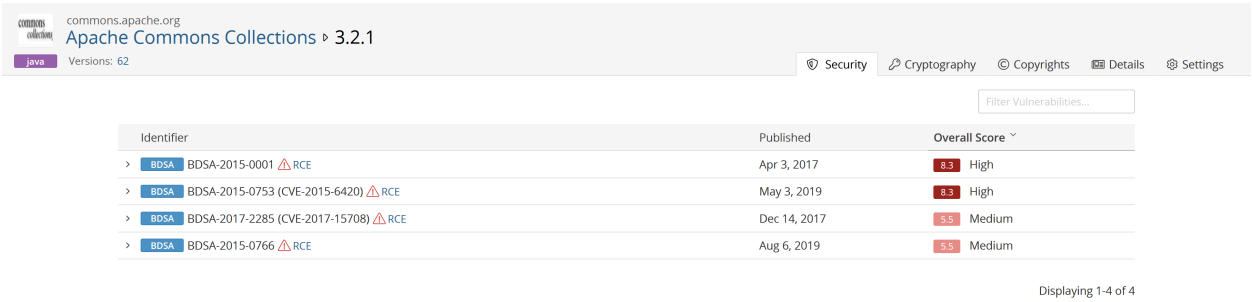
- 查看此组件版本的操作风险：

- 按与此组件版本相关的严重性级别从左到右查看每个严重性级别的漏洞数量：严重、高、中和低。

  上一个漏洞日期是此组件的漏洞上次在 Black Duck 中更新（由 Black Duck 知识库或用户更新）的日期。

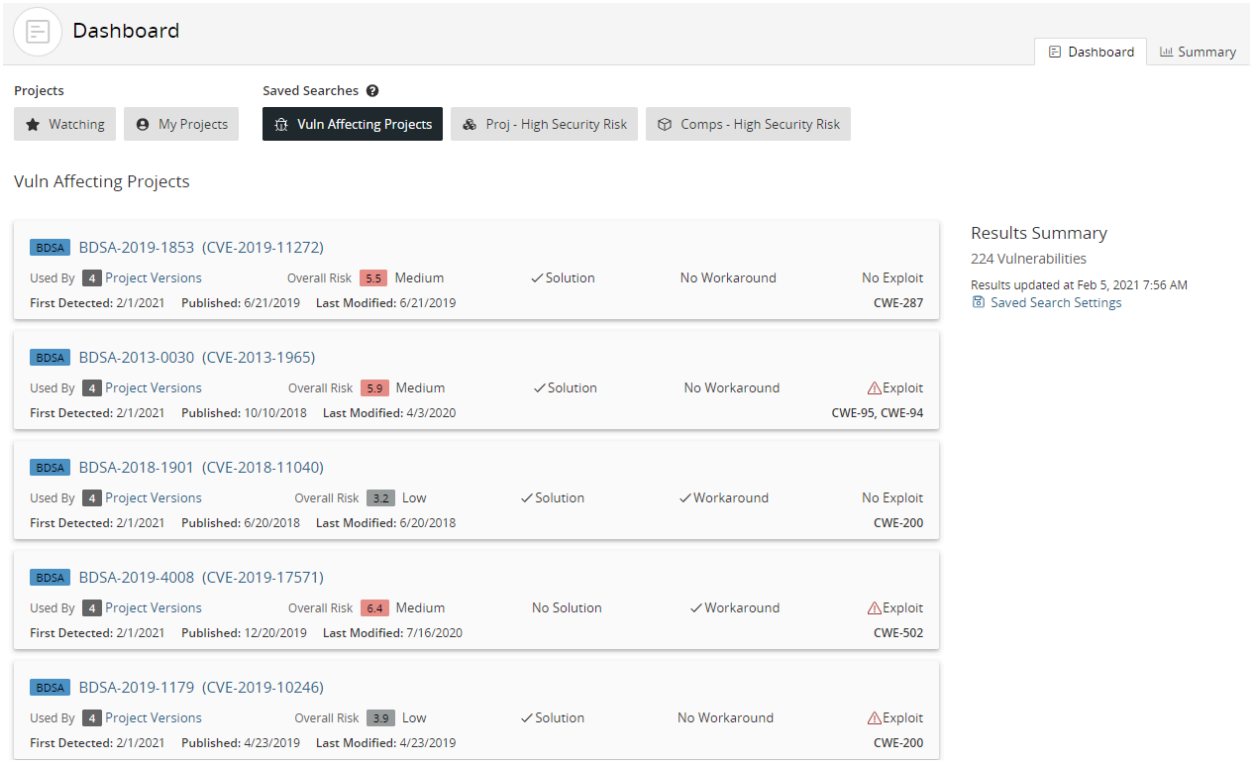
  选择一个值以显示 Black Duck KB 组件名称版本页面的安全选项卡，其中列出了与此组件版本关联的漏洞。

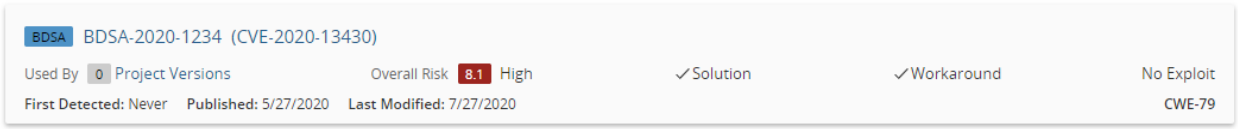
- 对于每个组件版本，搜索结果还会显示：
  - 审批状态。状态指示是否已审查此组件版本。
  - 首次检测日期。
  - 发布此组件版本的日期。
  - 较新版本的数量。
  - 组件的漏洞上次在 Black Duck 中更新（通过来自 Black Duck 知识库 的更新、用户手动更改关联的漏洞，等等）的日期。

- 管理组件在这些仪表板中的显示方式：
  - 使用排序依据字段选择要排序的属性，然后单击箭头以选择排序顺序 （升序）或 （降序）。
  - 使用过滤器字段过滤仪表板中显示的组件。

漏洞保存的搜索

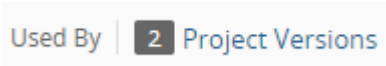


显示每个漏洞的以下信息：

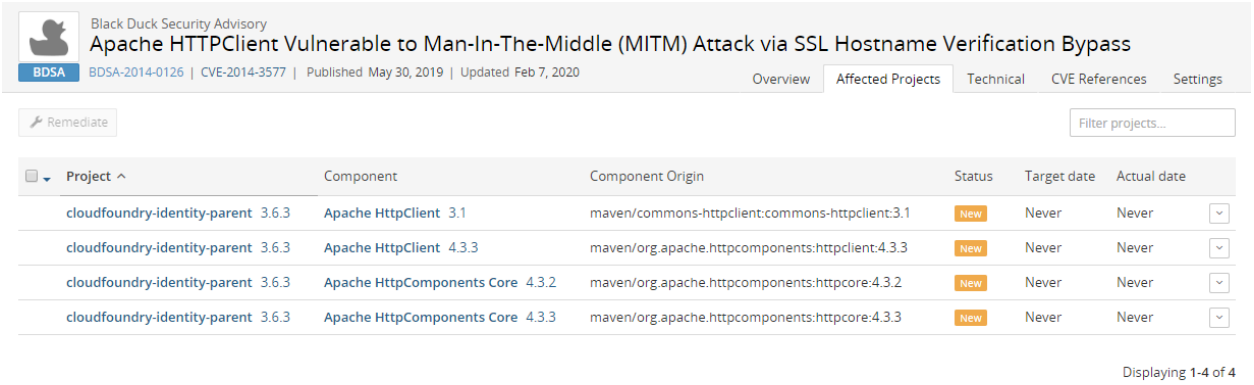


- 选择漏洞 ID 以查看有关漏洞的更多信息，比如其他分数值。您可以通过选择 CVE 编号查看国家漏洞数据库 (NVD) 信息，也可以通过选择 BDSA 编号查看 Black Duck 安全咨询 (BDSA) 信息。

- 在使用者旁边查看受此漏洞影响的项目版本数。

  选择项目版本以打开漏洞的受影响的项目选项卡，该选项卡列出了受此漏洞影响的项目版本。

- 查看总体风险分数。搜索结果显示 BDSA 漏洞的时间分数或 NVD 漏洞的基本分数以及相关风险级别。请注意，显示的分数和风险级别取决于选定的安全排名。

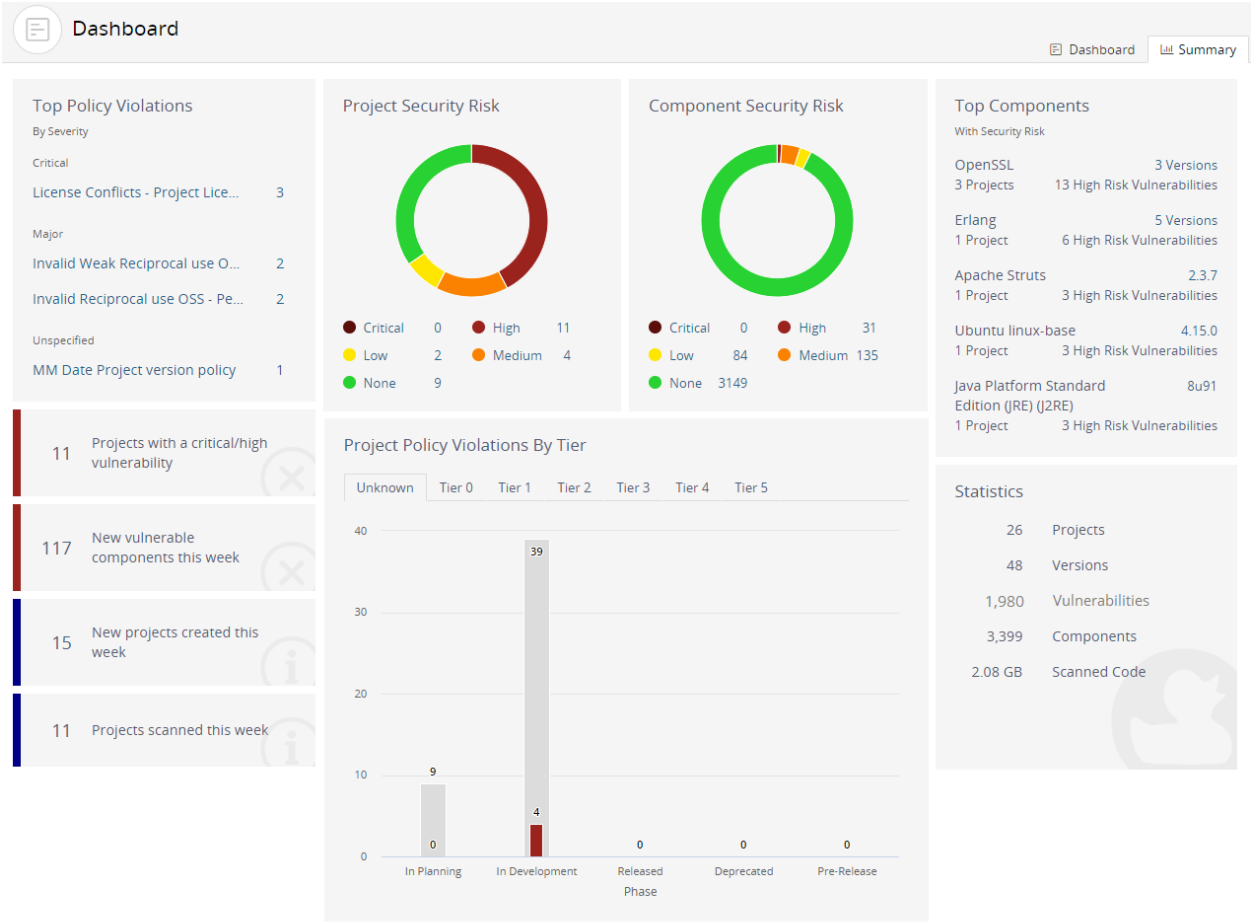
  选择分数以查看各个分数：时间、基本、可利用性和影响（适用于 BDSA）；基本、可利用性和影响（适用于 NVD）。
- 查看解决方案、解决方法或漏洞利用是否可用：
  - ✔ 表示存在可用于此漏洞的解决方案或解决方法。
  - ⚠ 表示存在此漏洞的利用。
- 对于每个漏洞，搜索结果还会显示：
  - 首次检测到。
  - 发布日期。
  - 上次修改日期。
  - 此安全漏洞的常见弱点枚举 (CWE) 编号。

导出到 CSV

您可以将仪表板导出到 CSV，从而将各个行转换为表格数据。要执行此操作，请单击 按钮，然后选择 CSV。

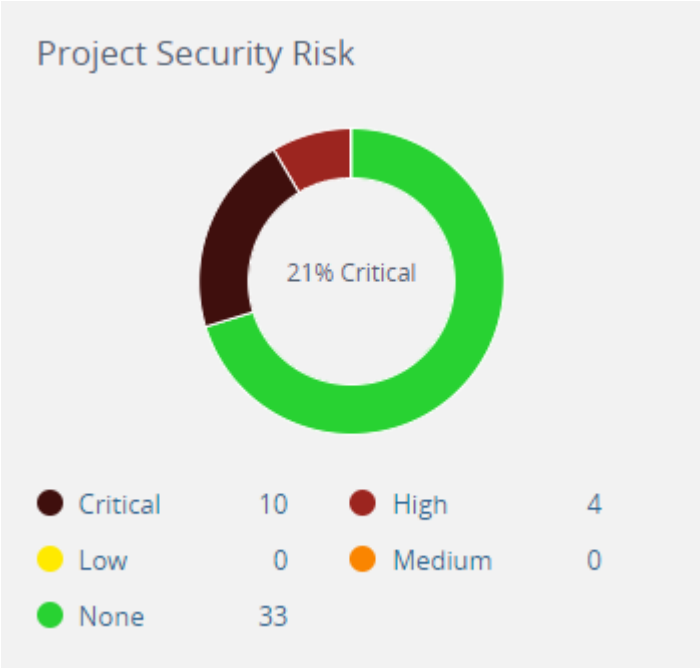
查看项目的运行状况

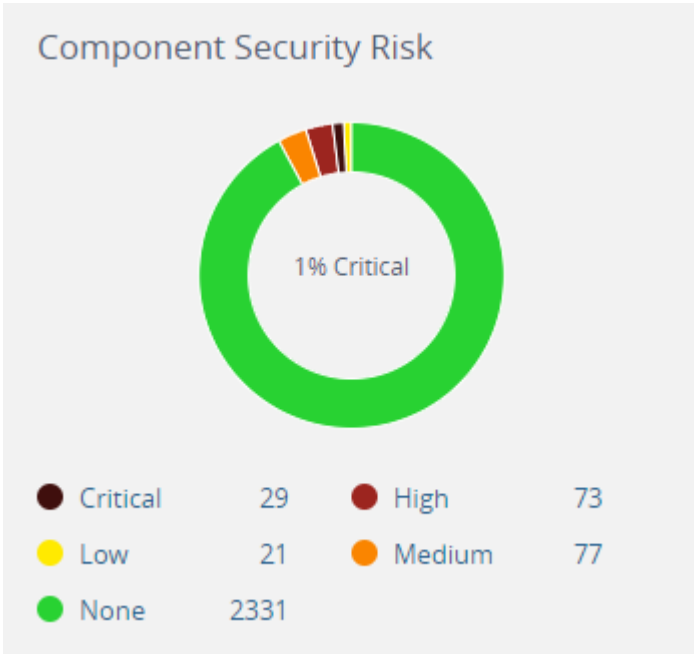
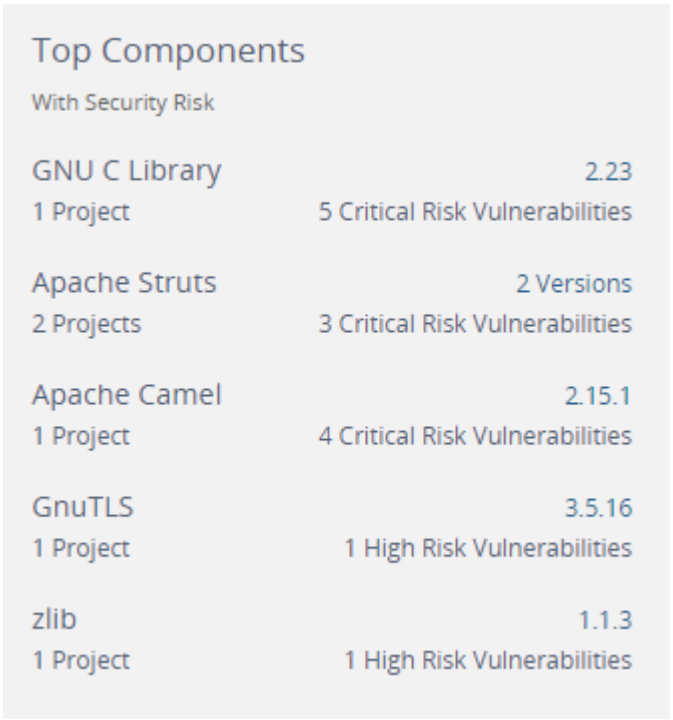
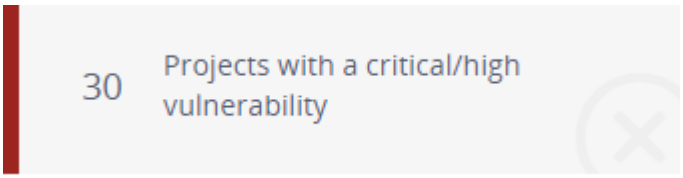
使用摘要选项卡查看项目的整体运行状况并确定关注的领域。该页面包含提供业务关键信息的小部件，您可以使用这些信息快速评估需要关注的领域。

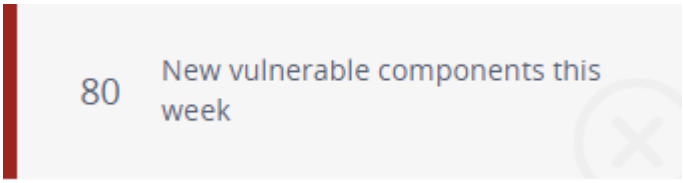
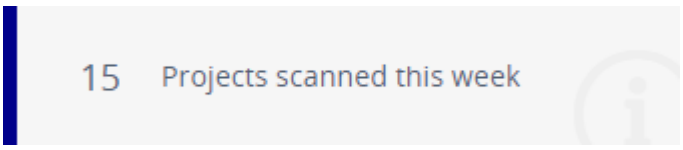
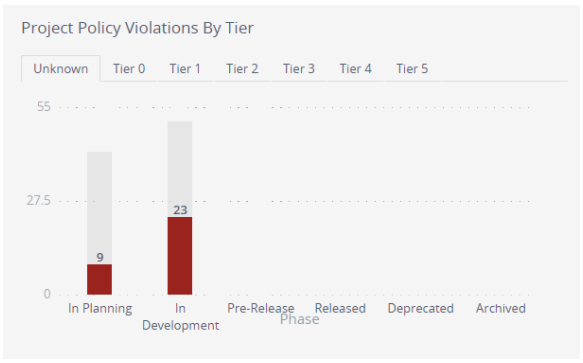


注: 摘要选项卡仅显示您有权查看的项目的信息。

下表介绍了摘要选项卡上显示的每个小部件，以及如何查看其他信息（如果可用）。请注意，显示的安全风险值使用 CVSS v2 或 CVSS v3.x 分数，具体取决于您选择的安全风险计算；默认情况下，将显示 CVSS v3.x 分数。请注意，如果您选择了 CVSS v2，图形将显示值为 0 的“严重”风险类别。

小部件	说明	更多信息
	主要策略违反小部件最多显示您有权查看的所有项目中的前五个策略违反。 策略规则按严重性级别列出，然后按策略违反数量按降序列出。如果策略规则没有为其分配严重性级别，小部件将按违反数量的降序显示前五个策略违反。 • 如果您没有“策略管理”模块，此小部件将不会显示在页面上。 • 如果您有“策略管理”模块，但没有配置任何策略规则或存在任何策略违反，则会显示一条消息。	选择一个策略规则以查看我的项目选项卡，该选项卡已过滤以显示有版本违反该策略规则的项目。
	项目安全风险小部件显示在每个安全风险级别您有权查看的项目数。请注意，此小部件统计项目的最高安全风险级别，而不是影响项目的所有安全级别。例如，如果项目具有中低安全风险，则将其视为具有中等安全风险的项目；它不统计为低安全风险的项目。	将鼠标悬停在图形上可查看具有该安全风险级别的项目数。

小部件	说明	更多信息
	组件安全风险小部件显示在每个安全风险级别您有权查看的项目中的组件数量。 请注意，小部件仅统计组件的最高安全风险。例如，如果某个组件具有中低安全风险，它将被视为一个具有中等安全风险的组件。	将鼠标悬停在图形上可查看具有该安全风险级别的组件数。
	具有安全风险的主要组件小部件最多显示您有权查看的项目中使用的前五个组件。为每个组件显示的信息包括： • 项目中使用的组件名称和版本数。如果只使用一个版本，则此处列出该特定版本。 • 具有此组件的项目数。 • 此组件中的安全风险数量，具有此处列出的最高安全风险。 组件按安全风险进行组织，风险最高的组件首先列出。	选择特定版本或版本数以查看 “组件版本详细信息” 页面。
	项目具有严重/高风险漏洞小部件显示版本包含严重和/或高安全风险组件的项目数量。	不适用。

小部件	说明	更多信息
	本周新的易受攻击组件小部件显示 Black Duck KB 过去七天（包括今天）内将漏洞映射到的组件数。	不适用。
	本周创建的新项目小部件显示您有权查看的过去七天（包括今天）内创建的项目数。	不适用。
	本周扫描的项目小部件显示包含过去七天（包括今天）的扫描的项目数。	不适用。
	按层级显示的项目策略违反小部件显示按阶段划分的具有策略违反的项目总数（按层级分组）。 • 如果您不为项目使用层级，则项目将分组在一个称为未知的类别中。 • 如果您没有“策略管理”模块，此小部件将按层级显示项目。	对于每一层，将鼠标悬停在条形图上，查看此阶段的项目数以及此阶段具有策略违反的项目数。
	统计小部件显示以下信息： • 项目列出了项目的数量。 • 版本列出了项目的项目版本数。 • 漏洞列出了项目中的漏洞数量。 • 组件列出了项目中使用的组件数量，包括忽略的组件。 • 扫描的代码列出所有扫描的 GB 数量。	不适用。

关于安全风险

Black Duck 帮助安全和开发团队识别其应用程序中的安全风险。

通过将漏洞映射到您的开源软件，Black Duck 可以为您提供有关项目安全风险的高级概述信息，以及可用于调查和修复安全漏洞的安全漏洞详细信息。

漏洞通过常见漏洞和披露编号 (CVE)（国家标准和技术研究所 (NIST) 维护的国家漏洞数据库 (NVD) 中报告的编号）和/或通过 (BDSA) 编号（如果您已获得 Black Duck 安全咨询许可）与开源组件链接。请注意，Black Duck 会在报告和 UI 中同时显示这些编号，因为它们代表来自不同来源的相同漏洞。

安全风险级别

NVD 和 BDSA 使用常见漏洞评分系统 (CVSS)，该系统提供反映漏洞严重性的数字分数。然后，数字分数被转换为风险级别，以帮助您评估安全漏洞并确定其优先级。

Black Duck 为您提供查看 CVSS v2 或 CVSS v3.x 分数的选项。默认情况下，Black Duck 显示 CVSS v3.x 分数。

- CVSS v2 分数具有以下值：
  - 低风险：0.0 - 3.9
  - 中等风险：4.0 - 6.9
  - 高风险：7.0-10.0

  请注意，Black Duck 显示的漏洞得分为 0.0 表示没有风险。

  虽然 CVSS v2 没有“严重”风险类别，但 Black Duck UI 中的安全图形显示了“严重”风险类别。此类别将显示 CVSS v2 的值为 0。
- CVSS v3.x 分数具有以下值：
  - 无：0.0
  - 低风险：0.1 - 3.9
  - 中等风险：4.0 - 6.9
  - 高风险：7.0 - 8.9
  - 严重风险：9.0 - 10.0

  请注意，为 CVSS v3.x 显示的分数可以是 v3.0 或 v3.1 分数。

估计安全风险

通过查看按安全漏洞严重性类别排序的组件的所有版本并计算每个组件版本的每种严重性类别的最大漏洞计数，可以得出此估计风险统计。每种严重性类别的最大漏洞计数显示在安全风险物料清单上的“按严重性类别估计的安全风险”中。最高严重性类别计数可能参考不同的组件版本。例如：

- 1.1 版本有 2 个严重漏洞，3 个高风险漏洞，15 个中风险漏洞，4 个低风险漏洞
- 1.2 版本有 2 个严重漏洞，4 个高风险漏洞，12 个中风险漏洞，1 个低风险漏洞
- 对于未知版本的组件，按严重性类别估计的安全风险将在物料清单上返回 2 个严重漏洞，4 个高风险漏洞，15 个中风险漏洞，4 个低风险漏洞。

用户应选择应用程序中使用的准确版本，以查看准确的风险，而不是估计的风险。提供此估计风险信息的目的是帮助确定哪些组件需要首先审查。我们鼓励用户将估计风险信息与 BD 策略管理结合使用，以根据公司的安全策略进一步确定应优先考虑哪些组件。

注：所提供的信息只是统计数据估计。因此，估计的安全风险将没有 CVE 数据。

建议的工作流程

要使用 Black Duck 管理安全风险：

1. 在安全团队的协助下，确定您的安全风险策略。
2. 如有必要，具有系统管理员角色的用户可以定义默认的安全排名。

   请注意，安全排名还定义了漏洞在报告中的显示方式。根据可用的数据，该漏洞将显示为：BDSA (NVD) 或 NVD (BDSA)。例如，如果安全排名为 NVD2、BDSA2、BDSA3、NVD3，则：

   - 漏洞 A 仅具有 NVD3 的数据。此漏洞在报告中列为 NVD-1234-5678。
   - 漏洞 B 具有 NVD3 和 BDSA3 的数据。报告将其列为 BDSA (NVD)。
   - 漏洞 C 拥有所有数据。报告将其列为 NVD (BDSA)。
3. 创建在组件不符合安全策略时触发违反的策略。
4. 根据您的兴趣：
   - 使用摘要仪表板查看项目的整体运行状况并确定关注的领域。使用此页面快速评估您需要关注的领域。
   - 使用这些“仪表板”页面查看风险的高级概述：
     - 使用“关注”或“我的项目”仪表板查看所有项目的安全风险。
     - 创建保存的搜索以自定义“仪表板”页面上显示的信息，以查看您感兴趣的项目、组件和漏洞。
   - 使用这些页面获取项目版本级别信息：
     - 项目版本页面/组件选项卡也称为项目版本 BOM，用于查看特定于该项目版本且具有安全风险的组件。
     - 项目版本页面/安全选项卡，用于查看与项目版本中使用的组件相关的每个严重性的安全漏洞。
5. 调查漏洞和策略违反。有关安全漏洞的详细信息，请查看：
   - CVE 页面
   - BDSA 页面（如果您已获得 Black Duck 安全咨询 (BDSA) 许可）
6. 查看漏洞的严重性后，具有相应角色的用户可以更改安全漏洞的修复状态。
7. 监控任何新安全漏洞的通知。

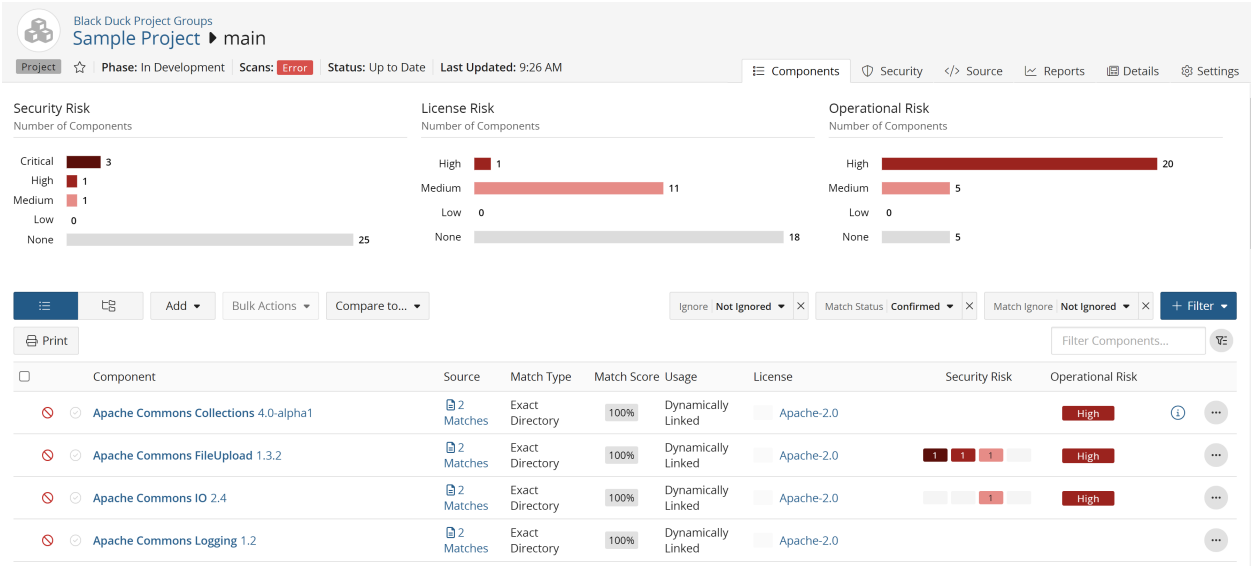
   如果针对一个或多个项目中包含的组件发布或更新了安全漏洞，您将收到通知警报。

5. 查看您的 BOM

将组件扫描 映射到项目版本后，结果将自动创建项目版本的 BOM。

要查看项目版本的 BOM：

1. 登录 Black Duck。
2. 使用正在关注或我的项目仪表板选择项目名称。此时将显示项目名称页面。
3. 选择要查看的项目的版本名称。
   组件选项卡显示 BOM。



默认情况下，BOM 显示组件的“平面”视图，找到的所有组件都在该视图中按同一级别列出。如果已启用分层 BOM，则会出现用于查看列表视图（如此处所示）或分层 BOM 的选项。选择树以查看基于文件系统关系的分层视图。

在 BOM 中调整组件和/或组件版本

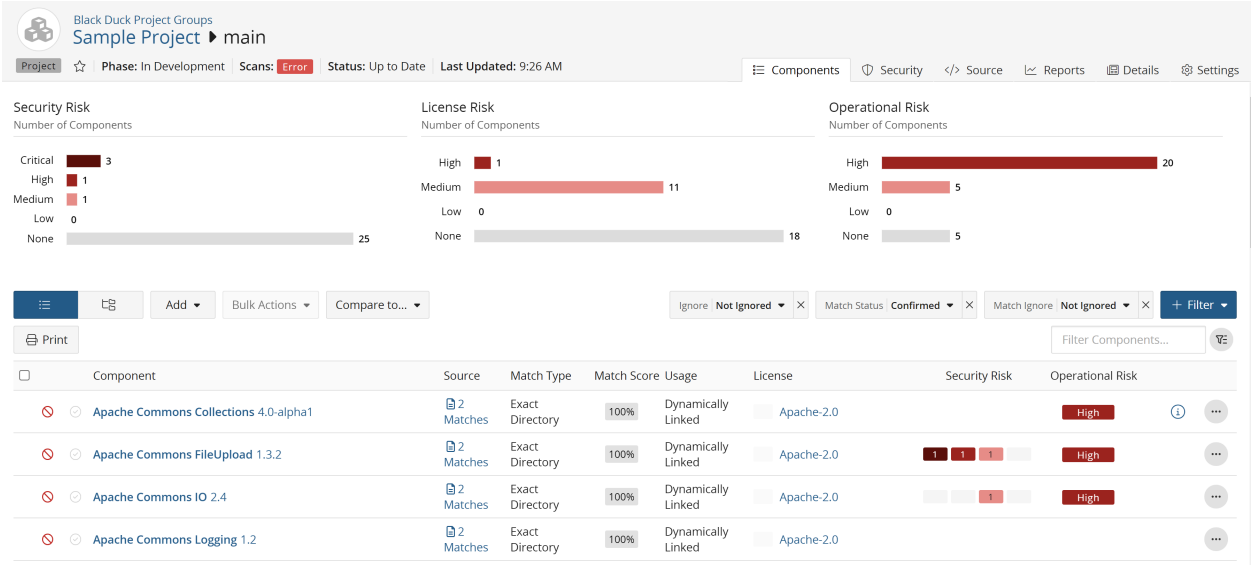
将组件扫描映射到项目版本后，扫描结果将自动创建项目版本的 BOM。虽然组件扫描通过将大多数存档文件中的组件与 Black Duck KB 中的组件进行比较，自动发现开源组件和组件版本，但您可能正在使用 Black Duck KB 中不可用的组件版本，或者您可能正在使用组件的修改版本。您可以在 BOM 中调整组件和组件版本。

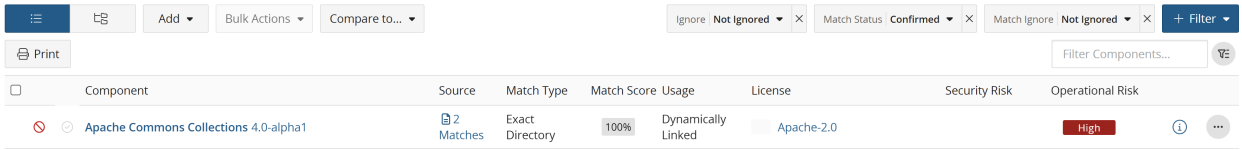
- 如果组件/版本在 Black Duck KB 中可用，具有相应角色的用户可以调整组件或组件版本，如下所述。
- 如果组件的组件版本在 Black Duck KB 中不可用，则具有“组件经理”角色的用户可以创建自定义版本并将其添加到 BOM 中。

要为 BOM 中的组件选择替代组件和/或版本匹配：

1. 登录 Black Duck。
2. 使用正在关注或我的项目仪表板选择项目名称。此时将显示项目名称页面。

3. 选择版本名称以打开组件选项卡并查看 BOM。



4. 在 BOM 的组件列表视图中，单击 并选择编辑以打开“编辑组件”对话框。
5. 在组件字段中键入 OSS 组件的名称，然后选择替代匹配项。
6. 从版本列表中选择组件的版本。该列表包含 Black Duck KB 中可用的组件的所有版本。
7. （可选）输入此调整的用途和/或选中修改复选框，并在字段中输入有关此修改的信息（可选）。
8. 单击保存。

   BOM 条目的组件和版本将被更新。信息指示符 ( ) 显示在表行中，表示组件和/或版本已从组件扫描中自动发现的版本更改：