BOMSkope

Netskope OSS Software

Version 1.0

🗂️ Overview

BOMSkope is a Software Bill of Materials (SBOM) manager designed and created by Netskope to streamline the process of tracking vulnerable software components across your vendors. By leveraging BOMSkope, organizations can gain visibility into their software supply chain and identify potential vulnerabilities before they become critical issues.

With BOMSkope, you can:

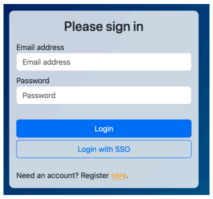
- **Upload and store SBOM submissions**: Seamlessly submit and manage SBOM files from various sources, ensuring you have a centralized repository for all your software component data.
- **Track components across vendors**: Gain visibility into the software components used by multiple vendors, allowing you to identify potential vulnerabilities and track changes in their dependencies.
- **Track vulnerability components across vendors**: Monitor vulnerable components across different vendors, enabling you to prioritize remediation efforts and reduce the attack surface of your organization.
- **Enhance security posture**: By providing visibility into software components and their associated vulnerabilities, BOMSkope helps you strengthen your organization's overall security posture and reduce the risk of attacks.

👥 Access Control

To access BOMSkope, simply navigate to your company's instance of the platform. You'll be prompted to log in at any time. If you're not automatically taken to the login screen, don't worry - just click the continue button and you'll be redirected to the login page.

Login

BOMSkope supports both local and SSO login. Depending on the method your company supports, log in with your credentials or through SSO by clicking on the “Login with SSO” button.



Please sign in

Email address

Email address

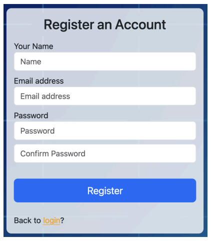
Password

Password

Need an account? Register here.

Register

If your company doesn't have an integration with Single Sign-On (SSO), you can still register for an account on the platform. To do so, click on the registration button on the sign-in page and provide the required information. Once you've completed the registration process, an administrator from the platform will need to review and approve your account before you can log in.



Register an Account

Your Name

Name

Email address

Email address

Password

Password

Confirm Password

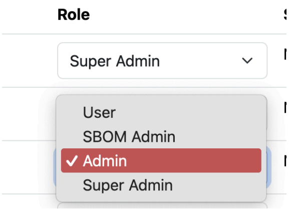
Register

Back to login?

Roles & Permissions

BOMSkope offers four distinct access levels to ensure secure and controlled access to the platform:

- **User**: A base-level account with read-only access, ideal for users who need to view information but not make changes.
- **SBOM Admin**: A level that grants you full control over the platform, including management of vendors, components, vulnerabilities, and more.
- **Admin**: Similar to SBOM Admin, this level offers all the same permissions plus additional capabilities, such as user management, SSO configuration, API key creation, and platform/integration setting modification.
- **Super Admin**: This highest-level access is similar to an Admin account, but it cannot be deleted or modified by an Admin. It's perfect for superusers who need maximum control.



Role

Super Admin

User

SBOM Admin

✓ Admin

Super Admin

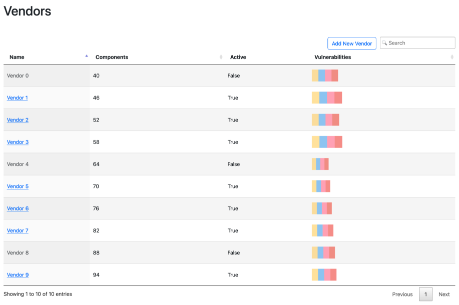
🏗️ The Platform

After logging into BOMSkope, you'll have access to four main sections: **Vendors, Components, Vulnerabilities, and Admin.**

Vendors

The Vendors section provides an overview of all your vendors, including their components and vulnerability counts by severity. Clicking into a vendor, you can:

- Explore the components and vulnerabilities associated with the vendor. Clicking into these items will provide you further details on them.



Vendors

Add New Vendor | Search

Name	Components	Active	Vulnerabilities
Vendor 0	40	False	
Vendor 1	46	True	
Vendor 2	52	True	
Vendor 3	58	True	
Vendor 4	64	False	
Vendor 5	70	True	
Vendor 6	76	True	
Vendor 7	82	True	
Vendor 8	88	False	
Vendor 9	94	True	

Showing 1 to 10 of 10 entries

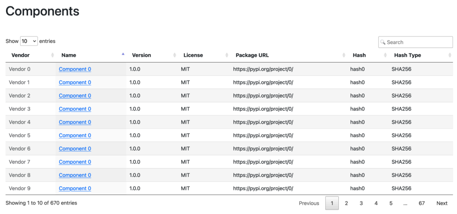
Previous 1 Next

- Modify vendor details or perform actions such as deleting the vendor’s data or the vendor itself. (Note: deletions **cannot** be recovered unless there is a backup of the database)
- Upload SBOM files to the vendor. Supported formats can be found in the Supported SBOM Formats section below.

Components

The Components section provides a centralized view of all components associated with your vendors. Here, you can:

- Browse an aggregated list of all components across your vendors
- Drill down into individual components to:
    - View detailed information about the component
    - Modify its details as needed
    - Delete the component



Components

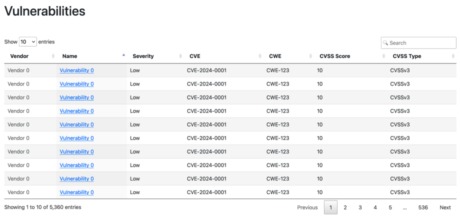
Vendor	Name	Version	License	Package URL	Hash	Hash Type
Vendor 0	Component 0	1.0.0	MIT	https://pypi.org/project/0/	hash0	SHA256
Vendor 1	Component 0	1.0.0	MIT	https://pypi.org/project/0/	hash0	SHA256
Vendor 2	Component 0	1.0.0	MIT	https://pypi.org/project/0/	hash0	SHA256
Vendor 3	Component 0	1.0.0	MIT	https://pypi.org/project/0/	hash0	SHA256
Vendor 4	Component 0	1.0.0	MIT	https://pypi.org/project/0/	hash0	SHA256
Vendor 5	Component 0	1.0.0	MIT	https://pypi.org/project/0/	hash0	SHA256
Vendor 6	Component 0	1.0.0	MIT	https://pypi.org/project/0/	hash0	SHA256
Vendor 7	Component 0	1.0.0	MIT	https://pypi.org/project/0/	hash0	SHA256
Vendor 8	Component 0	1.0.0	MIT	https://pypi.org/project/0/	hash0	SHA256
Vendor 9	Component 0	1.0.0	MIT	https://pypi.org/project/0/	hash0	SHA256

Showing 1 to 10 of 670 entries

Vulnerabilities

Similar to the Components section, the Vulnerabilities section provides a centralized view of all vulnerabilities associated with your vendors. Here, you can:

- Browse an aggregated list of all vulnerabilities detected from the components across your vendors
- Drill down into individual vulnerabilities to:
    - View details information about the vulnerability
    - Modify its details as needed
    - Delete the vulnerability (Note: The vulnerability may reappear if it is still present on the affected component; a solution to this is being evaluated)



Vulnerabilities

Vendor	Name	Severity	CVE	CWE	CVSS Score	CVSS Type
Vendor 0	Vulnerability 0	Low	CVE-2024-0001	CWE-123	10	CVSSv3
Vendor 0	Vulnerability 0	Low	CVE-2024-0001	CWE-123	10	CVSSv3
Vendor 0	Vulnerability 0	Low	CVE-2024-0001	CWE-123	10	CVSSv3
Vendor 0	Vulnerability 0	Low	CVE-2024-0001	CWE-123	10	CVSSv3
Vendor 0	Vulnerability 0	Low	CVE-2024-0001	CWE-123	10	CVSSv3
Vendor 0	Vulnerability 0	Low	CVE-2024-0001	CWE-123	10	CVSSv3
Vendor 0	Vulnerability 0	Low	CVE-2024-0001	CWE-123	10	CVSSv3
Vendor 0	Vulnerability 0	Low	CVE-2024-0001	CWE-123	10	CVSSv3
Vendor 0	Vulnerability 0	Low	CVE-2024-0001	CWE-123	10	CVSSv3
Vendor 0	Vulnerability 0	Low	CVE-2024-0001	CWE-123	10	CVSSv3

Showing 1 to 10 of 5,360 entries

Admin

Only users with the ‘Admin’ or ‘Super Admin’ role can see this section.

The Admin section is where you can perform elevated tasks on the platform. This section in itself is divided into four sections: **User Management, SSO Setup, Token Management, and Settings.**

User Management

The User Management section allows you to manage user accounts with ease. Here, you can:

- Update a user’s role
- Reset a user’s password
- Approve or deny pending user registrations
- And more, all in one convenient location

Some actions may be limited if the user is configured through SSO. It should be noted that users will **not** be automatically removed from the platform if removed from the SSO platform.

SSO Setup

In this section, you can customize settings for your SSO integration. You can also modify these values directly within the platform code by editing the `.env` file.

Currently, we support OpenID Connect (OIDC) as our SSO protocol. We're actively exploring the possibility of adding SAML support in the future.

Token Management

Here, you can create and manage API tokens to be utilized with our public API. For further information on this, refer to the code repository.

Settings

In this section, you can perform two key functions: upload a new logo and modify configuration settings for integrations.

- Upload a new logo to give your platform a fresh visual identity.
- Modify integration configurations to suit your needs. For further details on the integrations, see the Integrations section below.

🤝 Integrations

BOMSkope offers four different types of integrations: **OpenID Connect (OIDC), Google OSV, NIST NVD, and Bitsight VRM (formerly ThirdPartyTrust).**

OpenID Connect (OIDC)

BOMSkope supports OpenID Connect (OIDC) for secure Single Sign-On (SSO) configurations. You can set up SSO at any time through the Admin section in our web platform or via the backend.

Notably, enabling SSO will not disable local user authentication, allowing you to maintain a break-glass account for emergency access if needed.

Google OSV

The Google OSV (Open Source Vulnerabilities) database is a comprehensive repository of open-source vulnerabilities, curated by Google and drawing information from multiple sources including GitHub, PyPI, Go, and Rust advisory databases. For more details on the OSV database, please visit https://osv.dev/.

This valuable resource serves as the primary means for detecting vulnerabilities in components associated with uploaded Software Bill of Materials (SBOM) files. Vulnerabilities will automatically be created that are detected through this method.

NIST NVD

The NIST NVD is a comprehensive database of public vulnerabilities, maintained by the United States government for nearly all publicly disclosed security issues. In BOMSkope, the NVD provides additional context and information about vulnerabilities detected through our integration with Google's OSV database.

Bitsight VRM (formerly ThirdPartyTrust)

Our integration with Bitsight VRM allows you to continue managing and collecting vendor requirements within their platform. Once set up, the integration will sync this data down to BOMSkope, enabling seamless visibility and analysis.

To utilize this integration effectively, ensure that a requirement is set up in Bitsight VRM for collecting SBOM files from vendors. This requirement should be applied to each vendor you want to collect SBOM files from, allowing their information to be synced with BOMSkope. When a supported SBOM file is uploaded by a vendor and marked as reviewed in the platform, it'll be automatically synced down to BOMSkope, where it will be uploaded and analyzed for vulnerabilities.

📊 Supported SBOM Formats

BOMSkope supports both the CycloneDX and SPDX standards in various file formats. In specific, these are:

CycloneDX: JSON & XML
SPDX: JSON & SPDX

Examples of these formats can be found below.

JSON

CycloneDX generated JSON files (filename.json)
SPDX files in JSON format (filename.spdx.json, filename.json)

Example 1 (CycloneDX):

```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.2",
  "serialNumber": "urn:uuid:b4f2954f-a96d-4578-9509-1ae2d6476209",
  "version": 1,
  "metadata": {
    "timestamp": "2020-08-02T21:27:04Z",
    "tools": [{
      "vendor": "CycloneDX",
      "name": "CycloneDX Maven plugin",
      "version": "2.0.2",
      "hashes": [
        {
          "alg": "MD5",
          "content": "9a7ed39bba6c03f85a88fe114e24e4ad"
        },
        {
          "alg": "SHA-1",
          "content": "04b39fce560f8a9609e5b5db6e605fc2ba2c5a42"
        },
        {
          "alg": "SHA-256",
          "content": "78522e385d01fc74cb6410abb22b2b0ed9b47c1124635d955179402928820b43"
        }
…
```

Example 2 (SPDX):

```
{
  "SPDXID" : "SPDXRef-DOCUMENT",
  "spdxVersion" : "SPDX-2.3",
  "creationInfo" : {
    "created" : "2022-10-23T15:44:16Z",
    "creators" : [ "Person: Gary O'Neall", "Tool: spdx-maven-plugin" ],
    "licenseListVersion" : "3.18"
  },
  "name" : "examplemaven",
  "dataLicense" : "CC0-1.0",
  "documentDescribes" : [ "SPDXRef-example" ],
  "documentNamespace" : "http://spdx.org/documents/examplemaven-0.0.1",
  "packages" : [ {
    "SPDXID" : "SPDXRef-junit",
    "copyrightText" : "UNSPECIFIED",
…
```

XML

CycloneDX generated XML files (filename.xml)

Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<bom xmlns="http://cyclonedx.org/schema/bom/1.2"
serialNumber="urn:uuid:b4f2954f-a96d-4578-9509-1ae2d6476209" version="1">
    <metadata>
        <timestamp>2020-08-02T21:27:04Z</timestamp>
        <tools>
            <tool>
                <vendor>CycloneDX</vendor>
                <name>CycloneDX Maven plugin</name>
                <version>2.0.2</version>
                <hashes>
                    <hash alg="MD5">9a7ed39bba6c03f85a88fe114e24e4ad</hash>
                    <hash alg="SHA-1">04b39fce560f8a9609e5b5db6e605fc2ba2c5a42</hash>
                    <hash
alg="SHA-256">78522e385d01fc74cb6410abb22b2b0ed9b47c1124635d955179402928820b43</hash>
                    <hash
alg="SHA-384">aff816bf691e4490d4e977386c21abaceb97b7ce502d88c35c52cfdb7a7e50310ecc70019582d8247a9
9626bc98ad16b</hash>
…
```

SPDX

Standard SPDX file format. (filename.spdx)

Example:

```
SPDXVersion: SPDX-2.2
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: main-src
DocumentNamespace: https://swinslow.net/spdx-examples/example3/main-src-v2
```

```
Creator: Person: Steve Winslow (steve@swinslow.net)
Creator: Tool: github.com/spdx/tools-golang/builder
Creator: Tool: github.com/spdx/tools-golang/idsearcher
Created: 2021-08-26T01:50:30Z
…
```