How to manage OSS license obligations and SBoM by SW360's new features

Presenters:
kouki1.hama@toshiba.co.jp,

Agenda

Introduce SW360 and New features

- ○ SW360 in General
- ○ License and Obligation Management
- ○ Management SBOM by SPDX format

Who is Presenting?

- ○ Kouki Hama (濵 功樹)

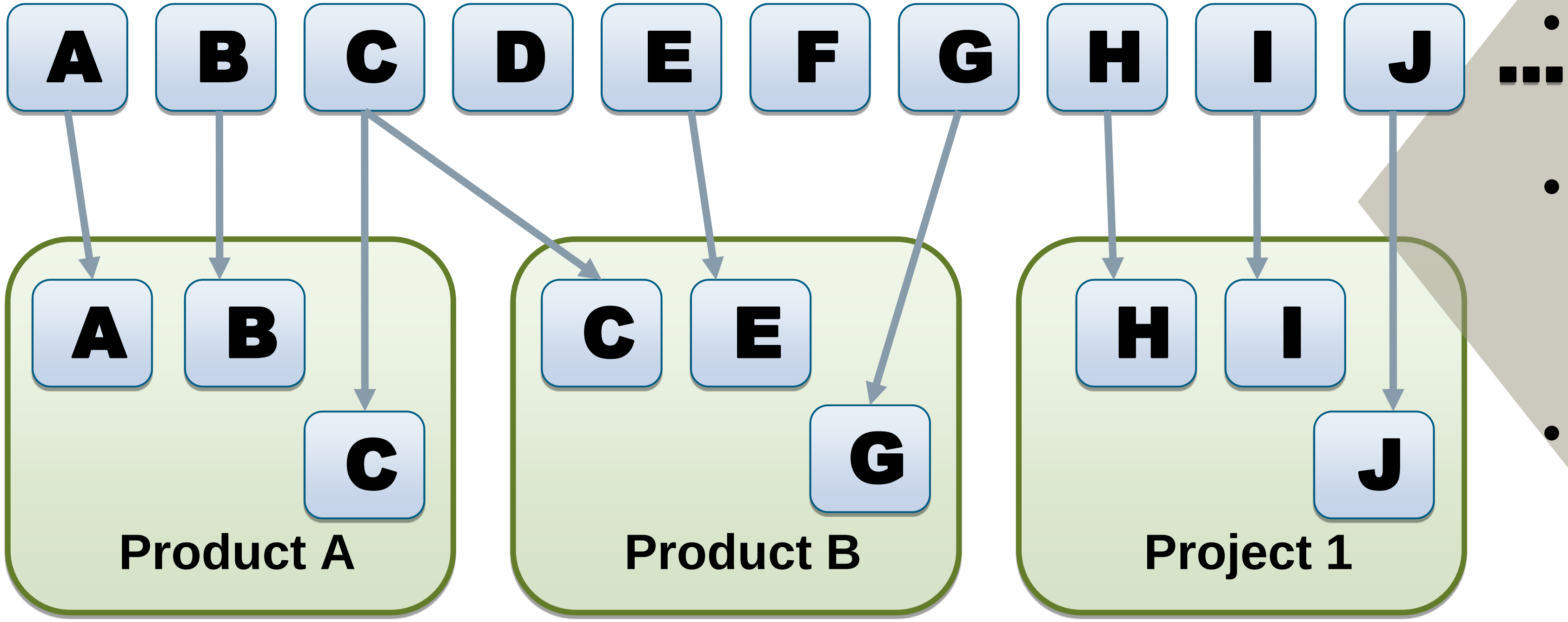
  Toshiba Corporation, Software Engineering & Technology Center

Overview

SW360 is a 3rd party software component catalogue

Assigns 3rd party and own components

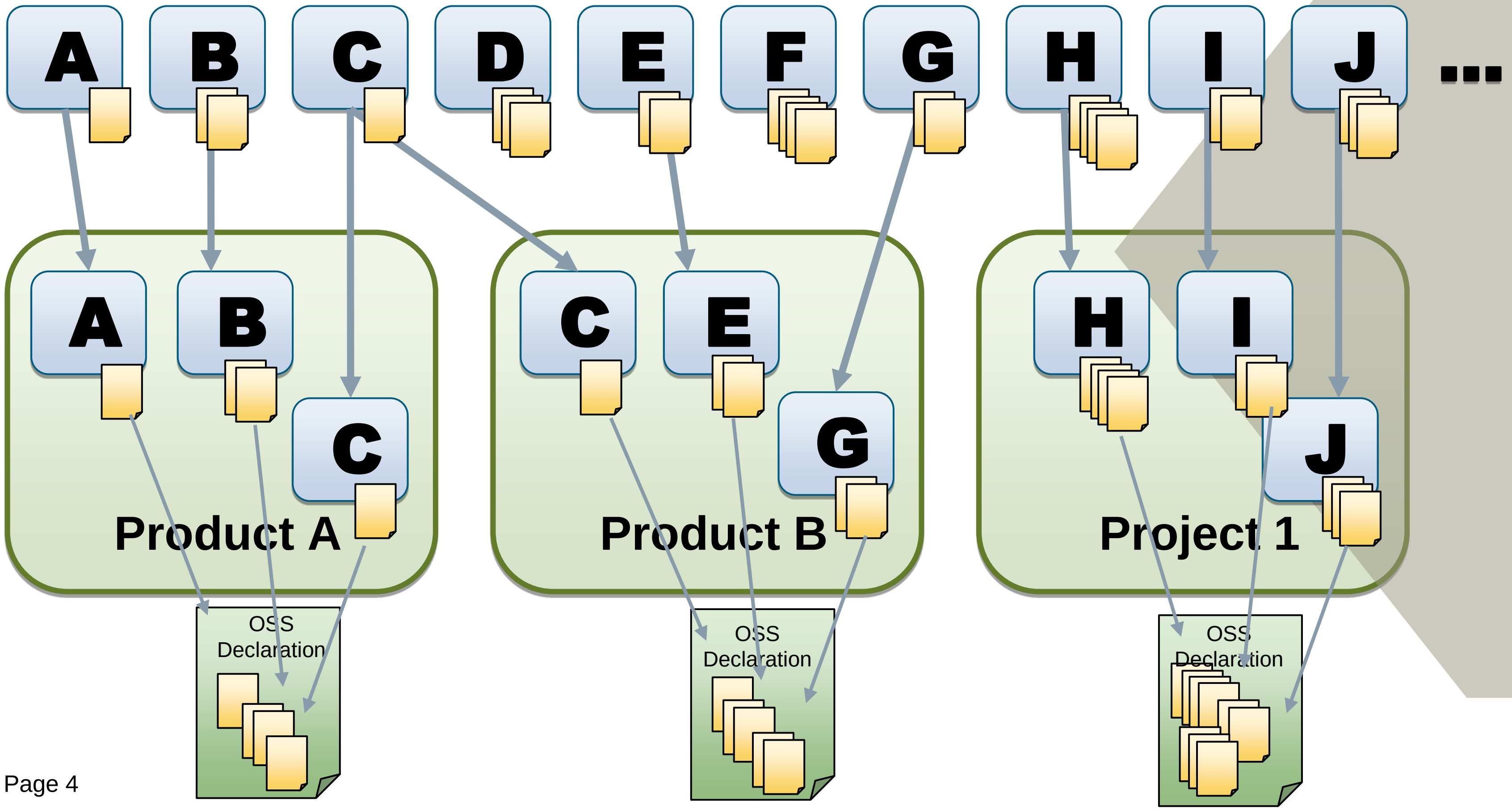
to products or projects



- **Goals and Benefits**
- Reuse information about components
- Coordinate product documentation process
- Supports OSS license clearing

Now for Licenses

All 3rd party and own components come with one or more licenses



- **License Information per Component**
- For each component license information is captured
- As such, license information per product is available

Manage OSS license and obligations

OpenChain Specification

- OpenChain ISO/IEC 5230 is the International Standard for open source license compliance.
- https://github.com/OpenChain-Project/Specification/blob/master/Official/en/2.1/openchainspec-2.1.pdf

- OpenChain Spec refers to license obligations

.

3.1.5 License obligations
A process shall exist for reviewing the identified licenses to determine the obligations, restrictions and rights granted by each license.

Manage OSS license and obligations

OSS License

- All OSS have licenses
- SPDX websites provides summary of OSS license info
  - https://spdx.org/licenses/

OSS License Obligations

- Different licenses have different obligations
- Some obligations should be managed by your companies or departments
- OSDAL (Open Source Automation Development Lab) Provides License obligation info
  - https://www.osadl.org/Access-to-raw-data.oss-compliance-raw-data-access.0.html

Import and Add license Obligations

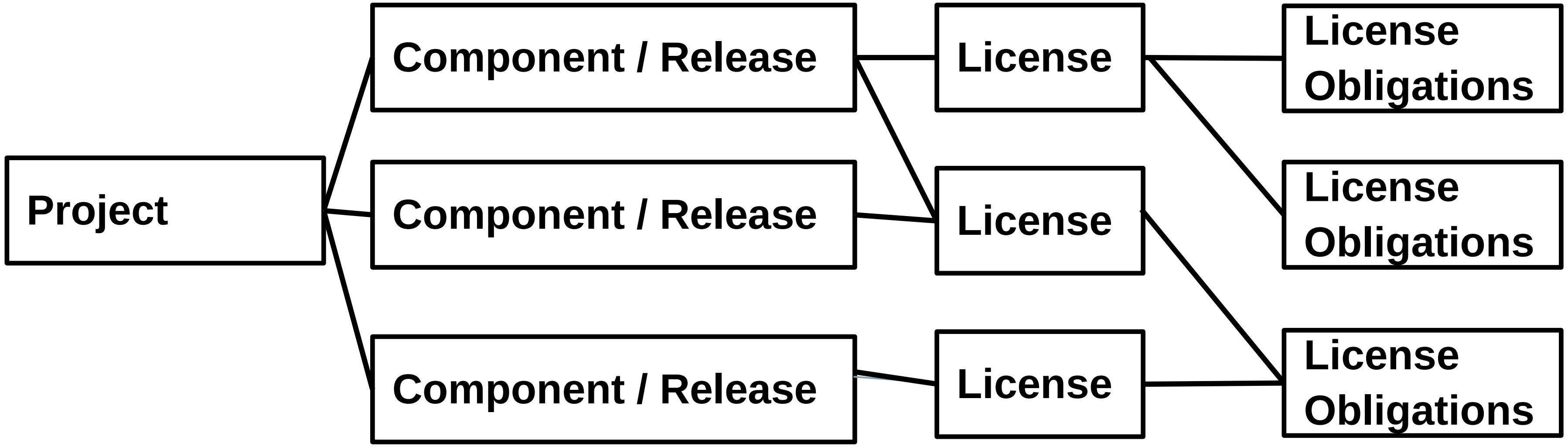
Import OSS license and Obligation info

- SW360 can import Licenses Data from SPDX through GUI
- SW360 can import Obligations Data from OSDAL through GUI

Add new obligation like OSDAL-like format

- Add new license obligations by yourself
- SW360 Supports to add license obligation
  by "input assistant function" or "elements of obligation”

Architecture Licensee / License Obligations



Licenses and Resulting Obligations
BSD-3-Clause Simple License Example

Copyright <YEAR> <COPYRIGHT HOLDER>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

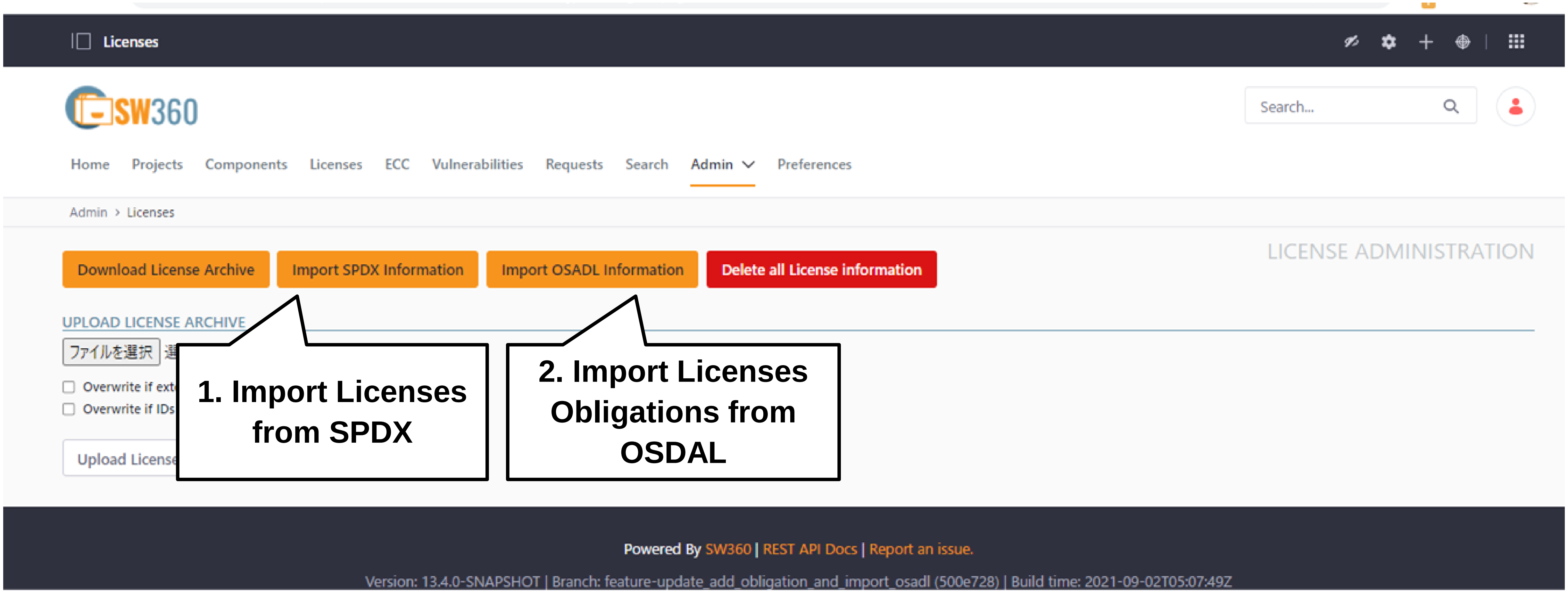
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE ...

- **USE CASE Source code delivery**
    - **YOU MUST Forward Copyright notices**
    - **YOU MUST Forward License text**
    - **YOU MUST Forward Warranty disclaimer**
    - **YOU MUST NOT Promote**
- **USE CASE Binary delivery**
    - **YOU MUST Provide Copyright notices In Documentation OR Distribution material**
    - **YOU MUST Provide License text In Documentation OR Distribution material**
    - **YOU MUST Provide Warranty disclaimer In Documentation OR Distribution material**
    - **YOU MUST NOT Promote**

Import License Obligation from OSDAL



1. Import Licenses from SPDX

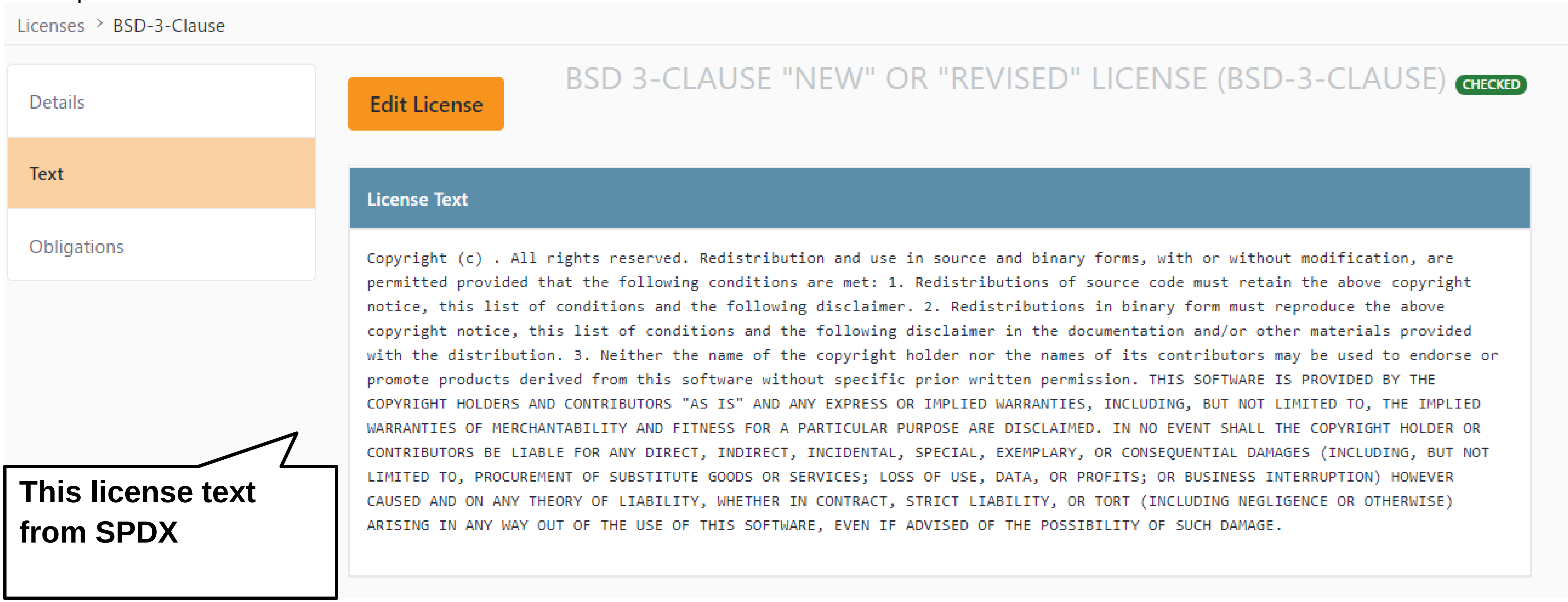
2. Import Licenses Obligations from OSDAL

Powered By SW360 | REST API Docs | Report an issue.

Version: 13.4.0-SNAPSHOT | Branch: feature-update_add_obligation_and_import_osadl (500e728) | Build time: 2021-09-02T05:07:49Z

License information in SW360

Example : BSD-3-Clause License text



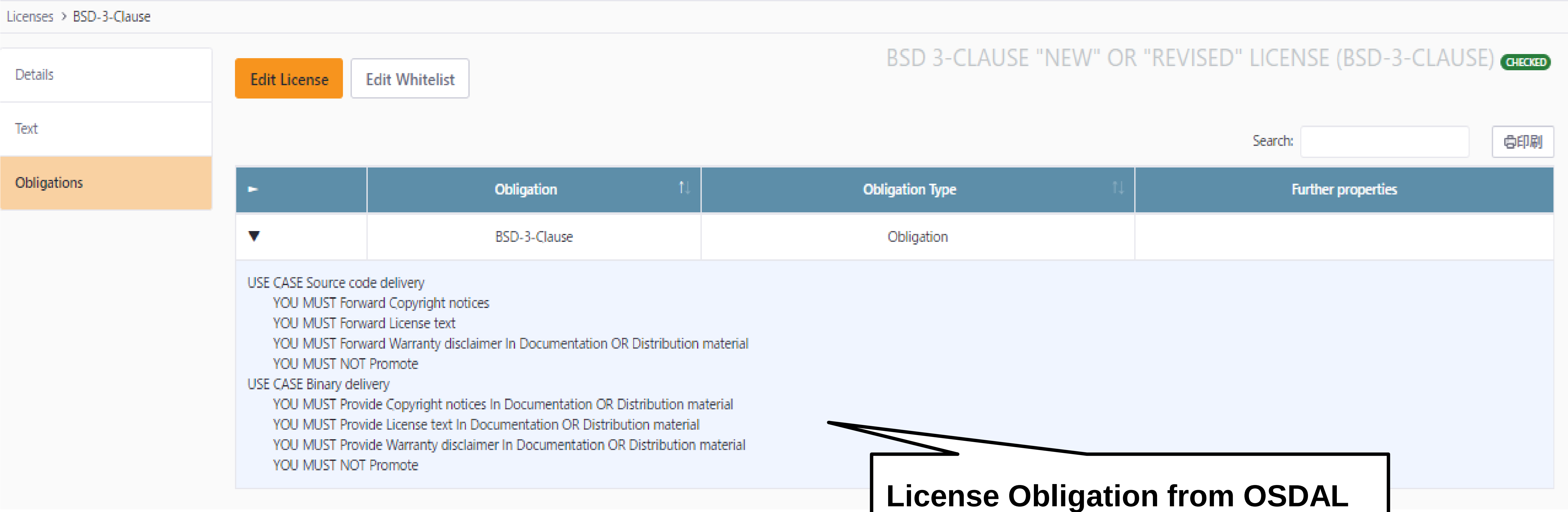
BSD 3-CLAUSE "NEW" OR "REVISED" LICENSE (BSD-3-CLAUSE)

License Text

Copyright (c) . All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This license text from SPDX

Importing results of License Obligations



Licenses > BSD-3-Clause

BSD 3-CLAUSE "NEW" OR "REVISED" LICENSE (BSD-3-CLAUSE) CHECKED

Search:

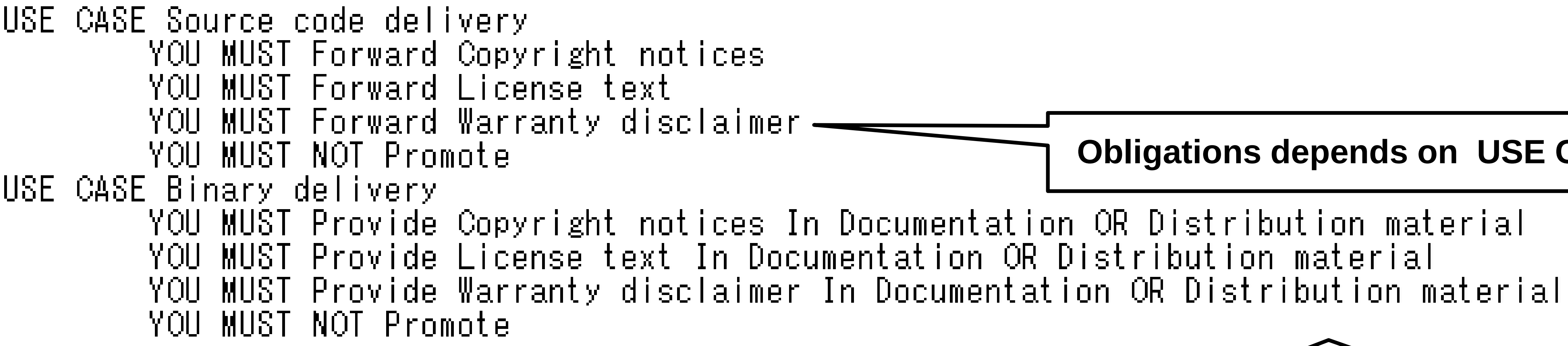
►	Obligation	Obligation Type	Further properties
▼	BSD-3-Clause	Obligation	

USE CASE Source code delivery
    YOU MUST Forward Copyright notices
    YOU MUST Forward License text
    YOU MUST Forward Warranty disclaimer In Documentation OR Distribution material
    YOU MUST NOT Promote
USE CASE Binary delivery
    YOU MUST Provide Copyright notices In Documentation OR Distribution material
    YOU MUST Provide License text In Documentation OR Distribution material
    YOU MUST Provide Warranty disclaimer In Documentation OR Distribution material
    YOU MUST NOT Promote

License Obligation from OSDAL

OSDAL licenses obligation

Example : BSD-3-Clause



```
USE CASE Source code delivery
        YOU MUST Forward Copyright notices
        YOU MUST Forward License text
        YOU MUST Forward Warranty disclaimer
        YOU MUST NOT Promote
USE CASE Binary delivery
        YOU MUST Provide Copyright notices In Documentation OR Distribution material
        YOU MUST Provide License text In Documentation OR Distribution material
        YOU MUST Provide Warranty disclaimer In Documentation OR Distribution material
        YOU MUST NOT Promote
```

Obligations depends on USE CASES

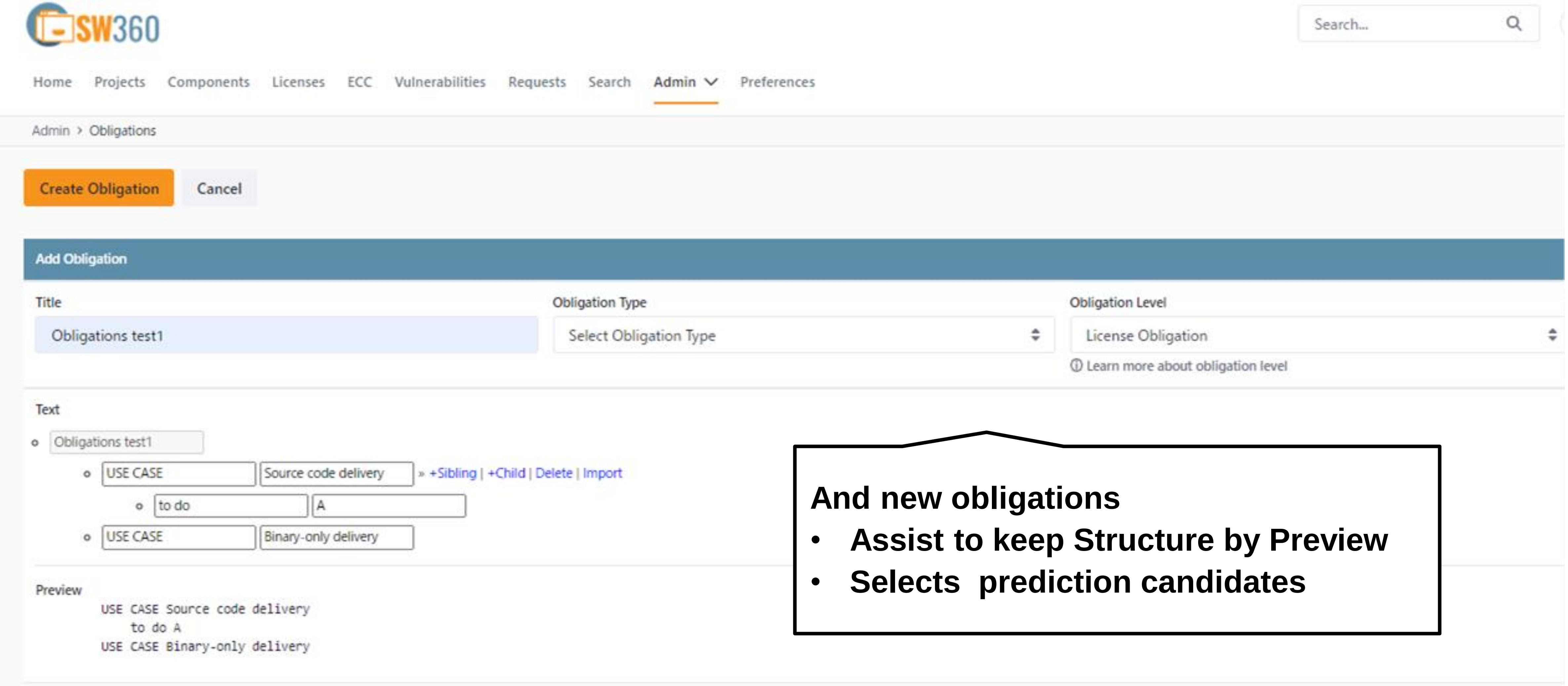
List of obligation items

And more. Such as

- **Patent hints**
- **COMPATIBILITY**
- **COPYLEFT CLAUSE**

https://www.osadl.org/fileadmin/checklists/unreflicenses/BSD-3-Clause.txt

Add New License Obligation Like OSDAL format



Title: Obligations test1

Obligation Type: Select Obligation Type

Obligation Level: License Obligation

ⓘ Learn more about obligation level

Text

- Obligations test1
  - USE CASE | Source code delivery » +Sibling | +Child | Delete | Import
    - to do | A
  - USE CASE | Binary-only delivery

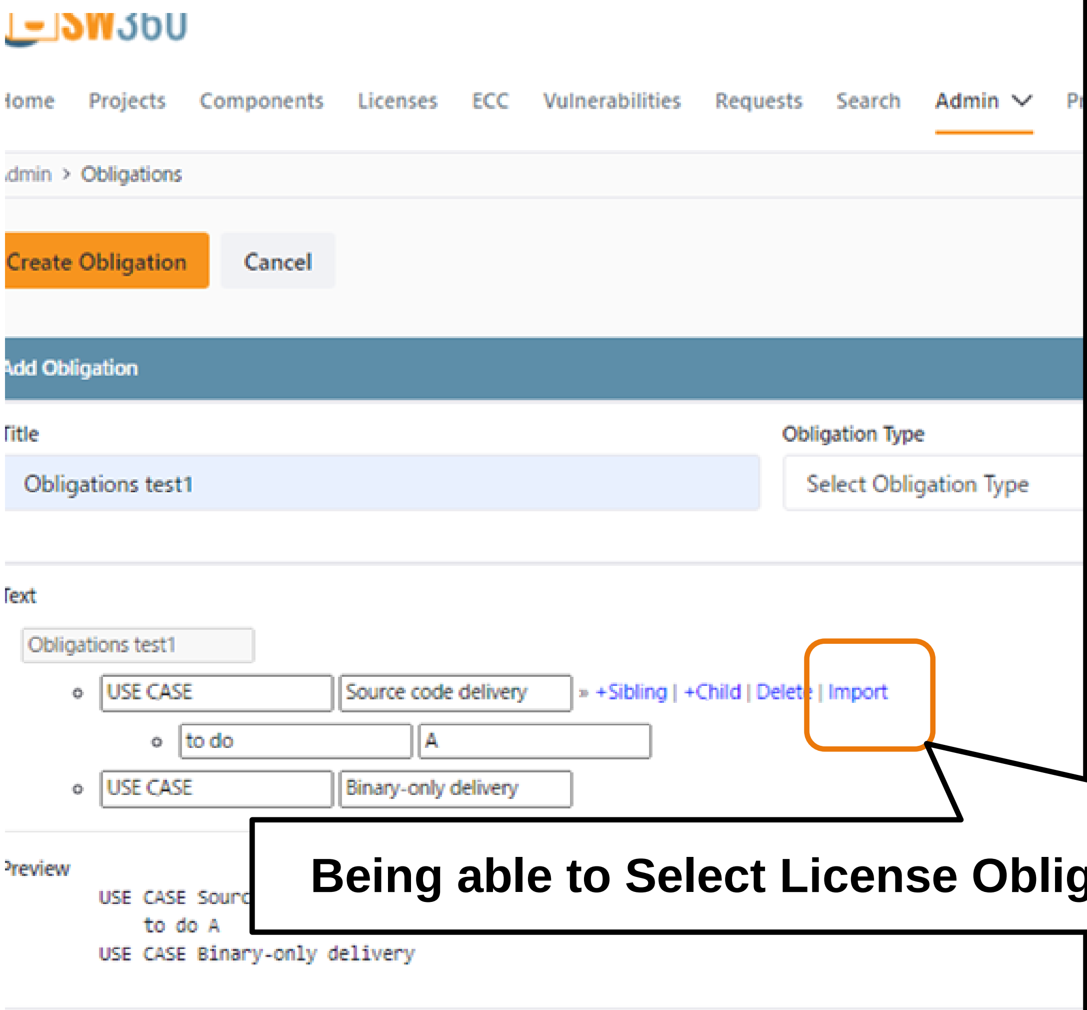
Preview

```
USE CASE Source code delivery
    to do A
USE CASE Binary-only delivery
```

And new obligations

- **Assist to keep Structure by Preview**
- **Selects prediction candidates**

Select Obligation Element



Home | Projects | Components | Licenses | ECC | Vulnerabilities | Requests | Search | Admin | Pr

Admin › Obligations

Create Obligation | Cancel

Add Obligation

Title: Obligations test1

Obligation Type: Select Obligation Type

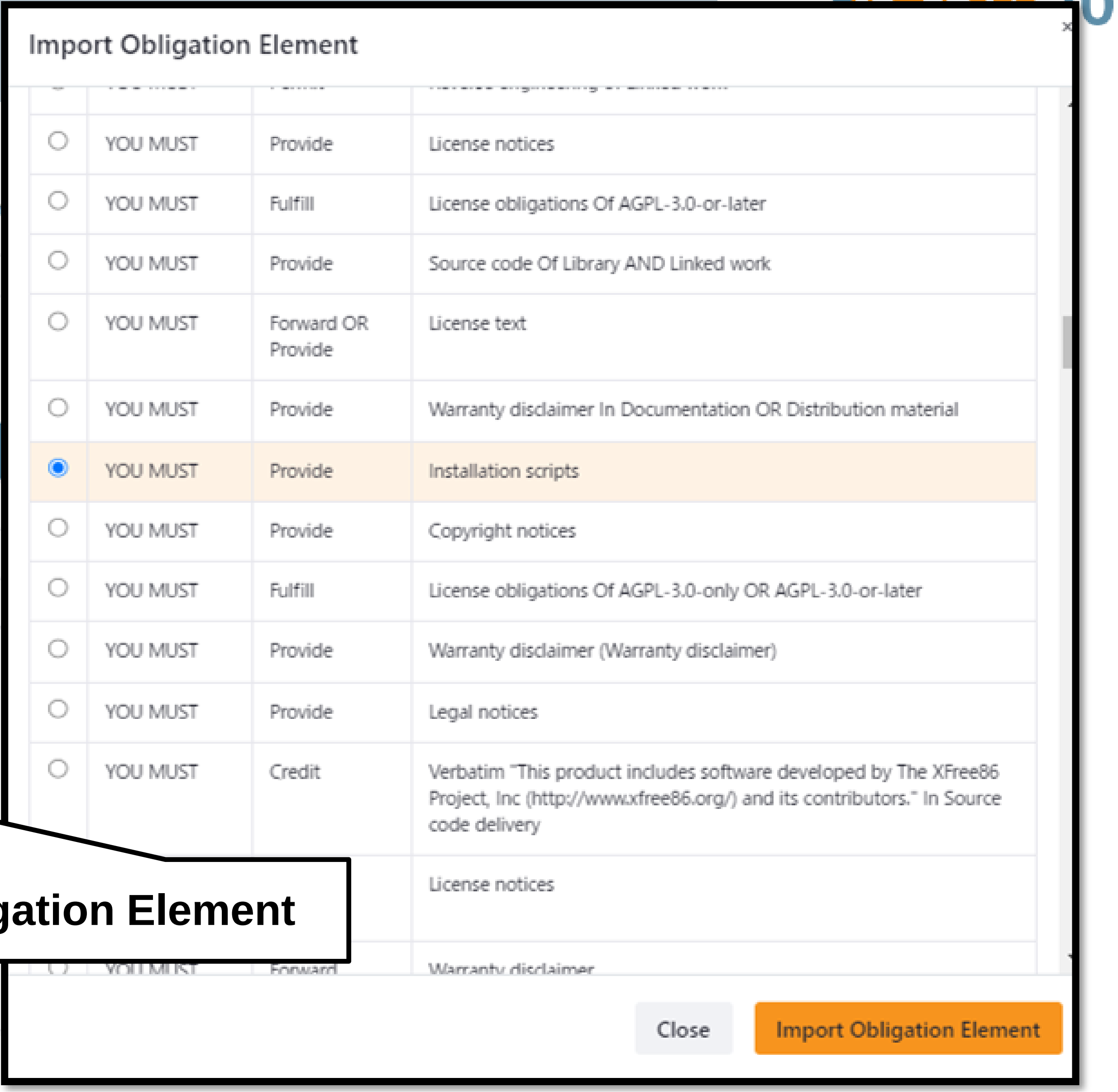
Text

Obligations test1

- USE CASE | Source code delivery » +Sibling | +Child | Delete | Import
  - to do | A
- USE CASE | Binary-only delivery

Preview

```
USE CASE Source code delivery
    to do A
USE CASE Binary-only delivery
```



Import Obligation Element

○	YOU MUST	Permit	Reverse engineering of Linked work
○	YOU MUST	Provide	License notices
○	YOU MUST	Fulfill	License obligations Of AGPL-3.0-or-later
○	YOU MUST	Provide	Source code Of Library AND Linked work
○	YOU MUST	Forward OR Provide	License text
○	YOU MUST	Provide	Warranty disclaimer In Documentation OR Distribution material
●	YOU MUST	Provide	Installation scripts
○	YOU MUST	Provide	Copyright notices
○	YOU MUST	Fulfill	License obligations Of AGPL-3.0-only OR AGPL-3.0-or-later
○	YOU MUST	Provide	Warranty disclaimer (Warranty disclaimer)
○	YOU MUST	Provide	Legal notices
○	YOU MUST	Credit	Verbatim "This product includes software developed by The XFree86 Project, Inc (http://www.xfree86.org/) and its contributors." In Source code delivery
			License notices
○	YOU MUST	Forward	Warranty disclaimer

Close | Import Obligation Element

Being able to Select License Obligation Element

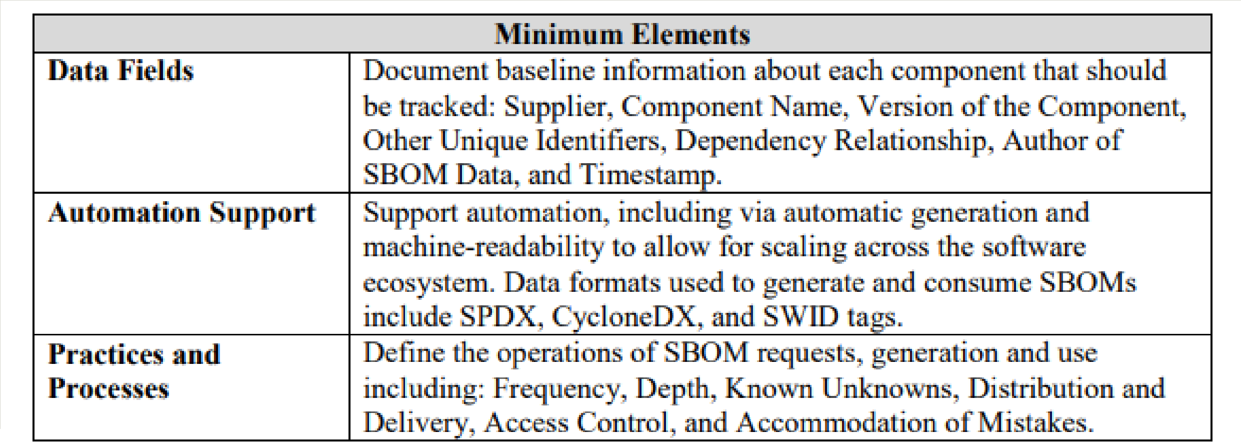
Manage Software Bill of Materials

Software Bill of Materials

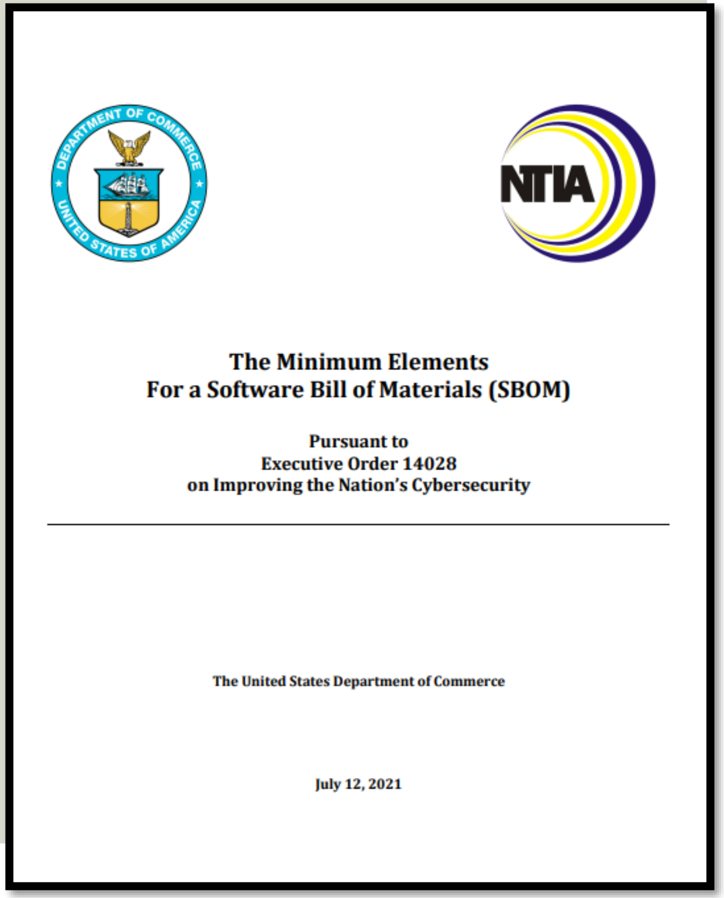
- OpenChain Spec refers to the (Software) Bill of Materials

3.3.1 Bill of materials
A process shall exist for creating and managing a bill of materials that includes each open source component (and its identified licenses) from which the supplied software is comprised.

- Executive Order 14028



Minimum Elements	
Data Fields	Document baseline information about each component that should be tracked: Supplier, Component Name, Version of the Component, Other Unique Identifiers, Dependency Relationship, Author of SBOM Data, and Timestamp.
Automation Support	Support automation, including via automatic generation and machine-readability to allow for scaling across the software ecosystem. Data formats used to generate and consume SBOMs include SPDX, CycloneDX, and SWID tags.
Practices and Processes	Define the operations of SBOM requests, generation and use including: Frequency, Depth, Known Unknowns, Distribution and Delivery, Access Control, and Accommodation of Mistakes.



The Minimum Elements
For a Software Bill of Materials (SBOM)

Pursuant to
Executive Order 14028
on Improving the Nation's Cybersecurity

The United States Department of Commerce

July 12, 2021

Manage Software Bill of Materials

SBoM Format

- **Software Package Data exchange (SPDX)**
- CycloneDX
- Software Identification (SWID) tags

SW360 Support

SPDX

- Software Package Data exchange
  - https://spdx.dev/
- ISO standard (ISO/IEC 5962:2021)

SPDX in SW360

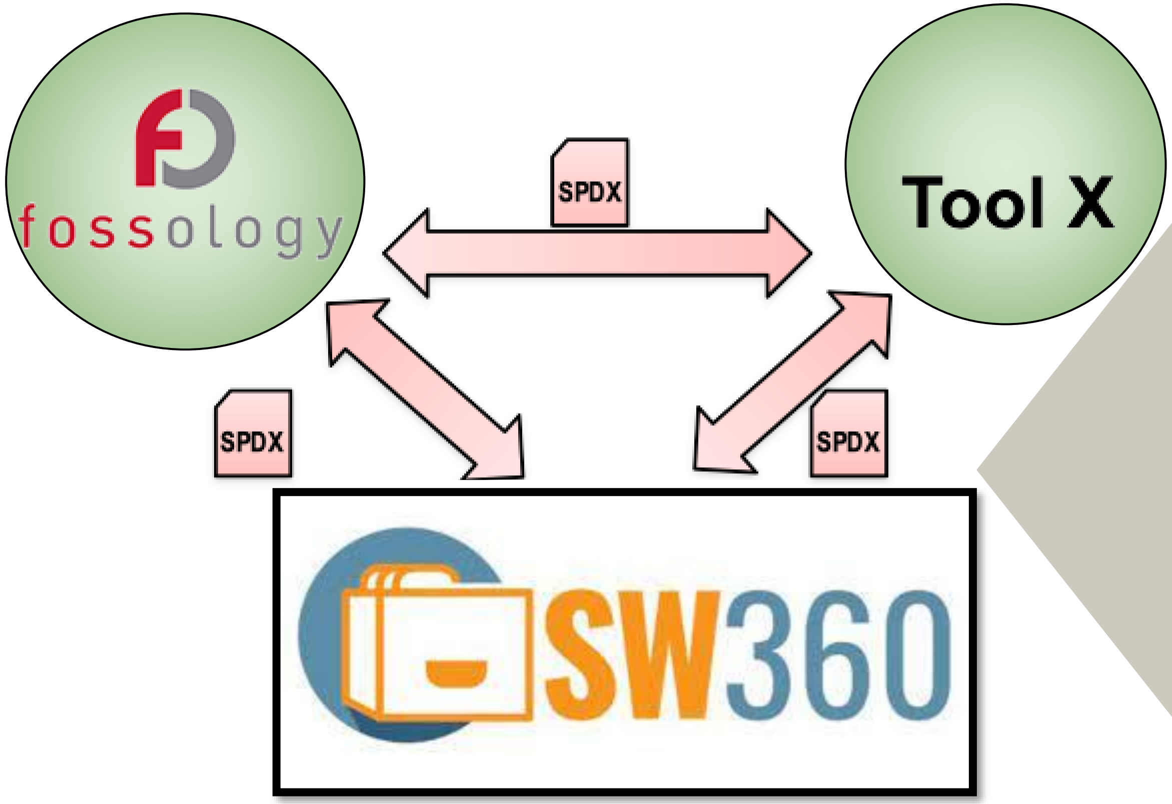
SPDX Clause

~~Clause 1: Scope~~
~~Clause 2: Normative references~~
~~Clause 3: Terms and definitions~~
~~Clause 4: Conformance~~
~~Clause 5: Composition of an SPDX document~~
Clause 6: Document Creation Information
Clause 7: Package Information
~~Clause 8: File Information~~
Clause 9: Snippet Information
Clause 10: Other Licensing Information Detected
Clause 11: Relationship between SPDX Elements Information
Clause 12: Annotation Information
~~Clause 13: Review Information (deprecated)~~

Plan to Support Clause 8 : file information

Now SW360 Supports
Clause 6, 7, 9, 10,11,12

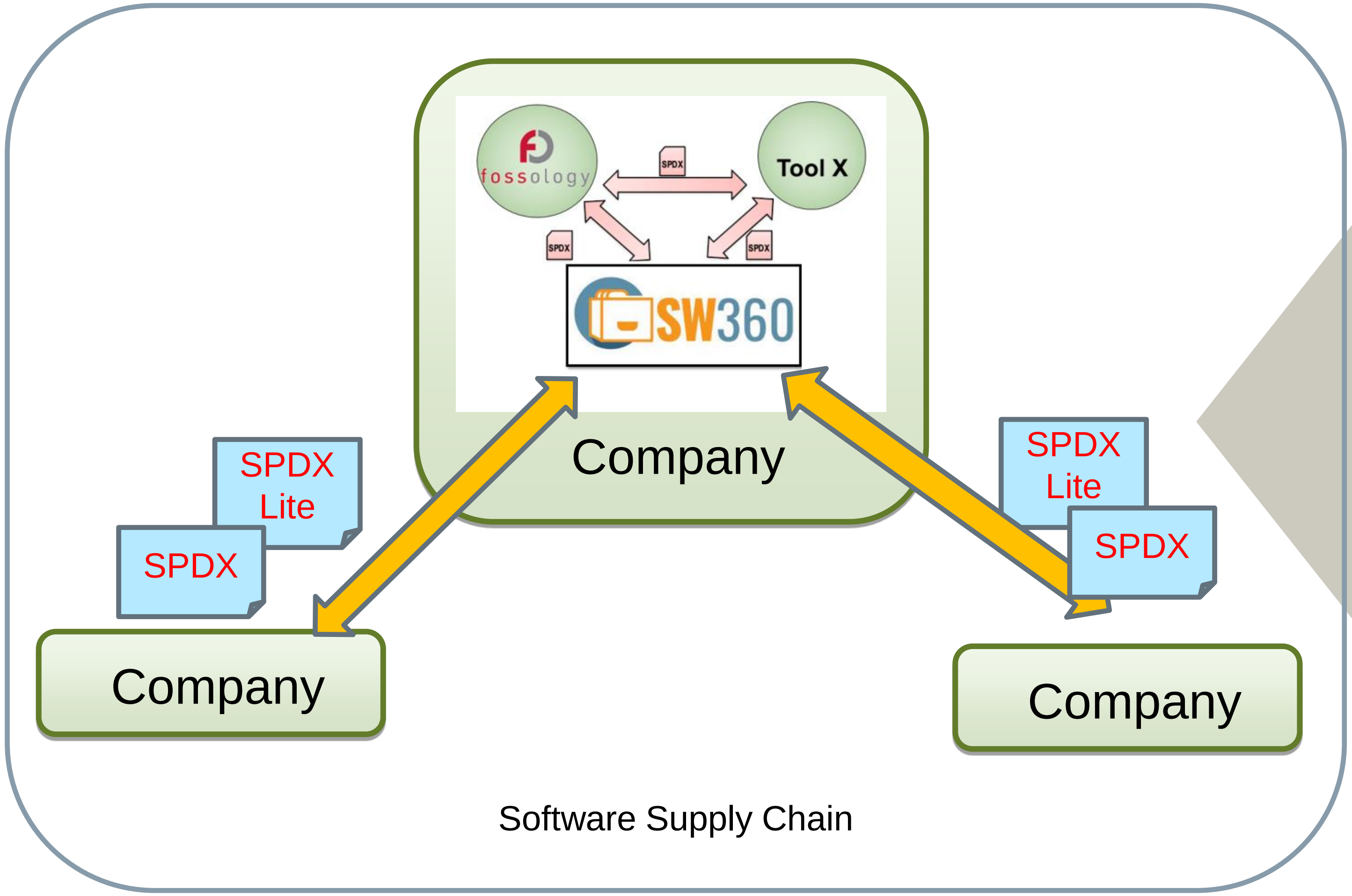
SPDX for Open Interconnectivity



Goals and Benefits

- Tool integration: exchange clearing information
- Open to partners
- Maximize reuse of available clearing information

SPDX Lite and SW360



SPDX Lite

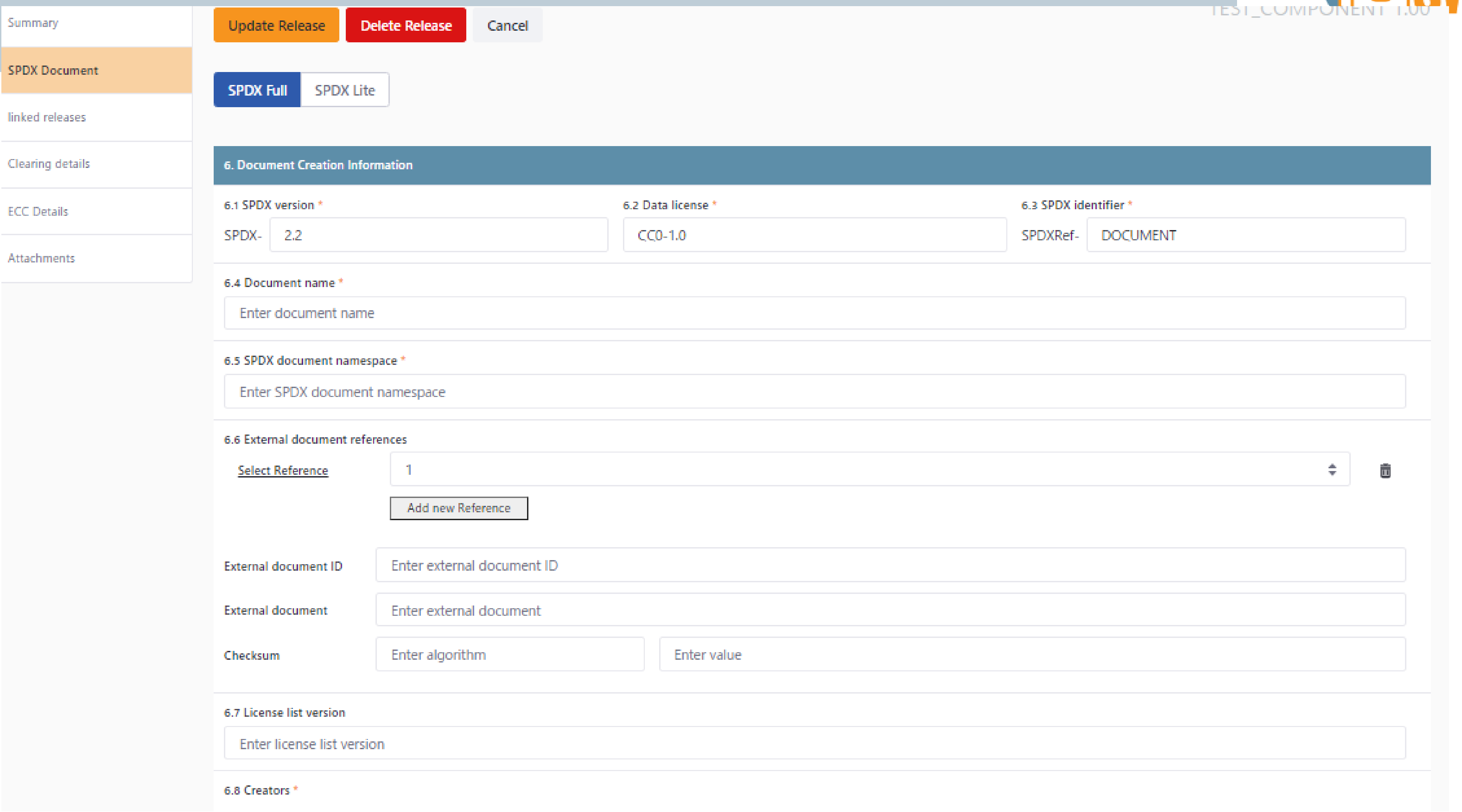
The SPDX Lite profile defines a subset of the SPDX specification, from the point of view of use cases in some industries. SPDX Lite aims at the balance between the SPDX standard and actual workflows in some industries.

SPDX Lite has affinity with SPDX tools due to its containing the mandatory part of the Document Creation and Package Information in the SPDX Lite definition.

An SPDX Lite document can be used in parallel with SPDX documents in software supply chains.

https://spdx.github.io/spdx-spec/SPDX-Lite/

Edit SPDX in SW360


TEST_COMPONENT 1.00

6. Document Creation Information

6.1 SPDX version *	6.2 Data license *	6.3 SPDX identifier *
SPDX- 2.2	CC0-1.0	SPDXRef- DOCUMENT

6.4 Document name *

Enter document name

6.5 SPDX document namespace *

Enter SPDX document namespace

6.6 External document references

Select Reference: 1

External document ID: Enter external document ID

External document: Enter external document

Checksum: Enter algorithm | Enter value

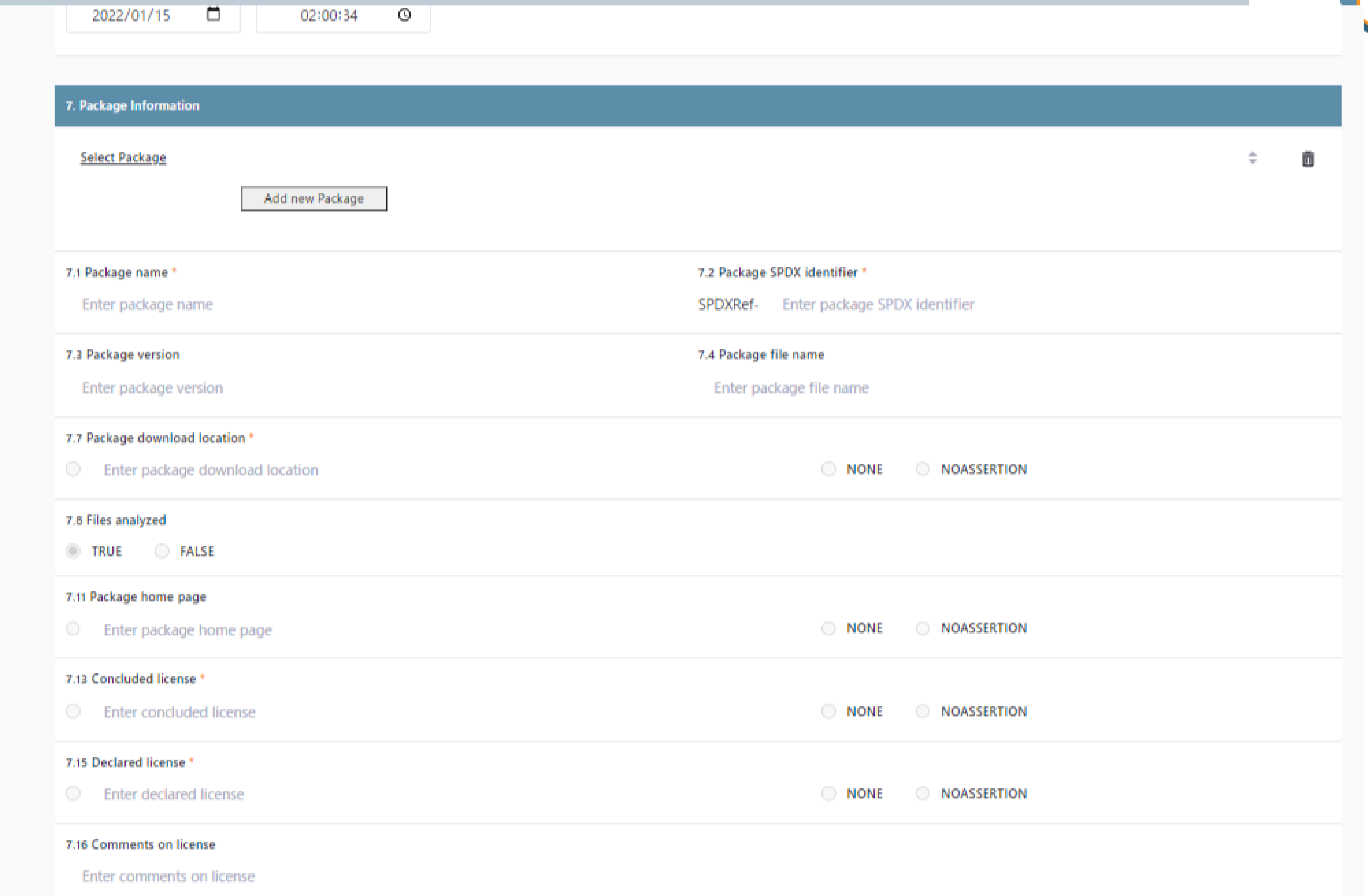
6.7 License list version

Enter license list version

6.8 Creators *

https://github.com/toshiba/sw360/commits/dev/feature-spdx_information_management

Edit SPDX in SW360



2022/01/15 02:00:34

7. Package Information

Select Package

Add new Package

7.1 Package name *

Enter package name

7.2 Package SPDX identifier *

SPDXRef- Enter package SPDX identifier

7.3 Package version

Enter package version

7.4 Package file name

Enter package file name

7.7 Package download location *

○ Enter package download location ○ NONE ○ NOASSERTION

7.8 Files analyzed

● TRUE ○ FALSE

7.11 Package home page

○ Enter package home page ○ NONE ○ NOASSERTION

7.13 Concluded license *

○ Enter concluded license ○ NONE ○ NOASSERTION

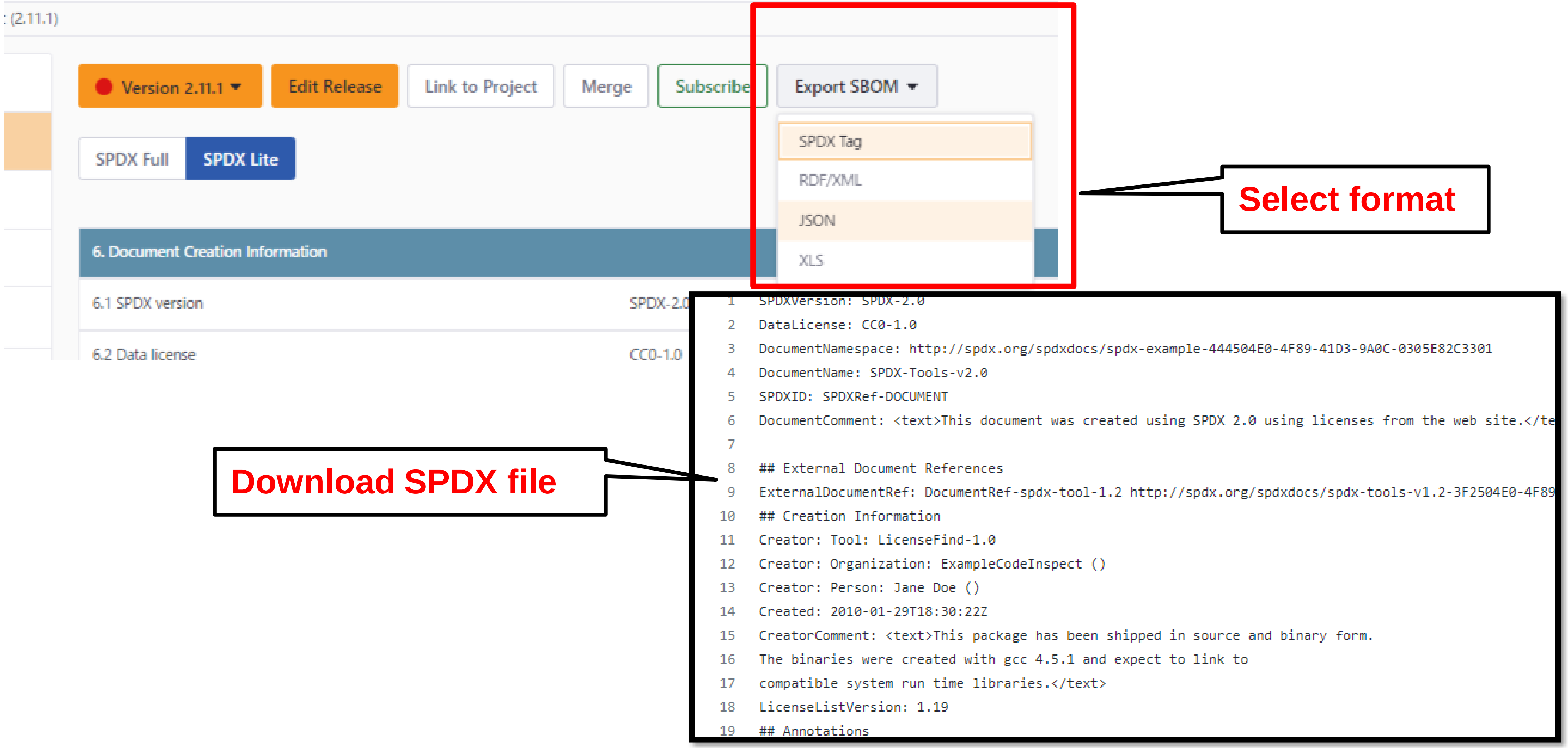
7.15 Declared license *

○ Enter declared license ○ NONE ○ NOASSERTION

7.16 Comments on license

Enter comments on license

Export SPDX



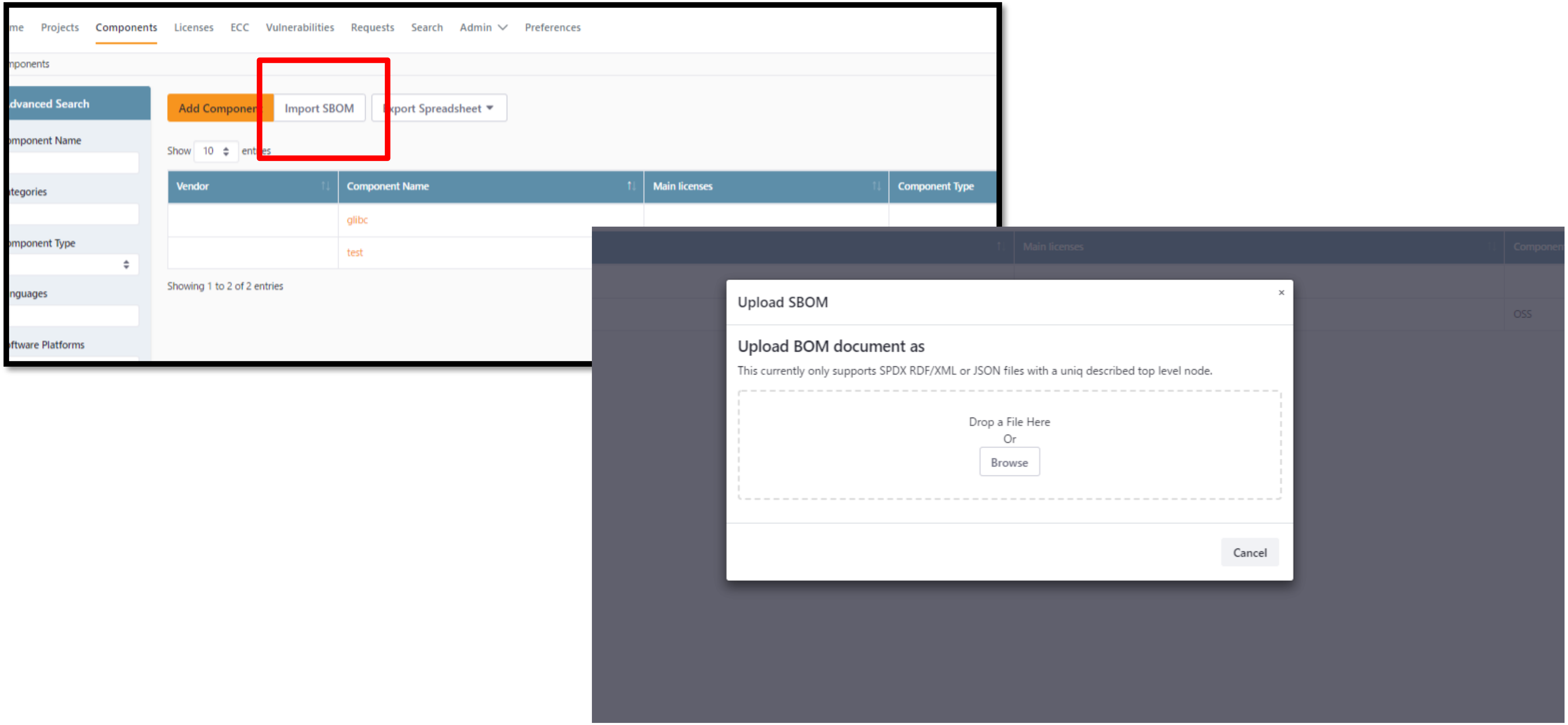
Select format

```
SPDXVersion: SPDX-2.0
DataLicense: CC0-1.0
DocumentNamespace: http://spdx.org/spdxdocs/spdx-example-444504E0-4F89-41D3-9A0C-0305E82C3301
DocumentName: SPDX-Tools-v2.0
SPDXID: SPDXRef-DOCUMENT
DocumentComment: <text>This document was created using SPDX 2.0 using licenses from the web site.</te

## External Document References
ExternalDocumentRef: DocumentRef-spdx-tool-1.2 http://spdx.org/spdxdocs/spdx-tools-v1.2-3F2504E0-4F89
## Creation Information
Creator: Tool: LicenseFind-1.0
Creator: Organization: ExampleCodeInspect ()
Creator: Person: Jane Doe ()
Created: 2010-01-29T18:30:22Z
CreatorComment: <text>This package has been shipped in source and binary form.
The binaries were created with gcc 4.5.1 and expect to link to
compatible system run time libraries.</text>
LicenseListVersion: 1.19
## Annotations
```

Download SPDX file

Import SPDX



Vendor	Component Name	Main licenses	Component Type
	glibc		
	test		

Showing 1 to 2 of 2 entries

Upload SBOM

Upload BOM document as

This currently only supports SPDX RDF/XML or JSON files with a uniq described top level node.

Summary

- SW360 is Software BoM management tool
- Managing Software BoM management is important for OSS compliance and OpenChain Specification
- New SW360 supports License obligations and SPDX format

Thank you!

Useful Links

- CC-BY-SA 4.0
  https://creativecommons.org/licenses/by-sa/4.0/
- **Internet**
  https://www.eclipse.org/sw360
- **GitHub**
  https://www.github.com/eclipse/sw360
  https://www.github.com/sw360
- **Further Links**
  https://www.spdx.org