SIEMENS

Ingenuity for life

FOSSology and SW360: Updates

Presenter: michael.c.jaeger@siemens.com

Siemens Corporate Technology

FOSSology and SW360

Component Analysis Tool

+

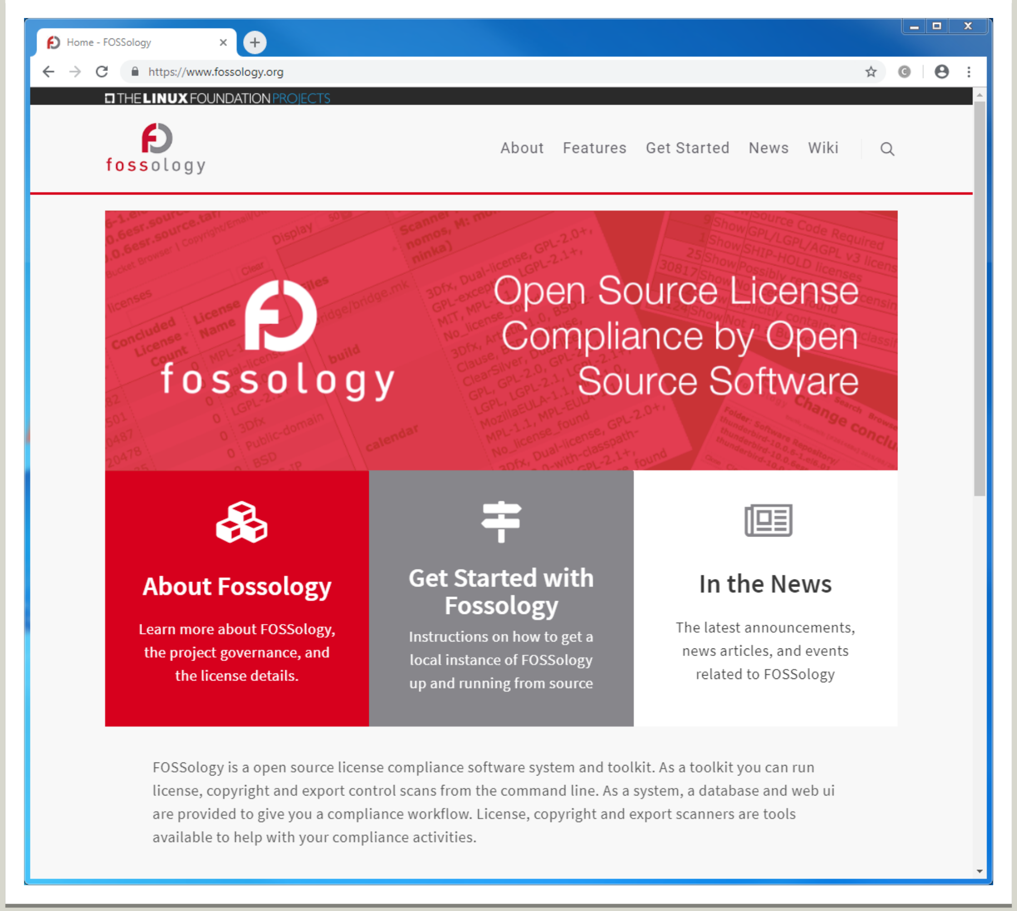
Software Catalogue

FOSSology – Linux Foundation Collaboration

SIEMENS

www.fossology.org

- 2008 initial publication by HP
- 2015 Linux Foundation Collaboration Project
- A Linux server application
- Different tasks for OSS license compliance
  - Scanning for licenses
  - Copyright, authorship, e-mails
  - ECC statements
  - Generation of documentation
  - Export and import SPDX files



Open Source License Compliance by Open Source Software

About Fossology

Learn more about FOSSology, the project governance, and the license details.

Get Started with Fossology

Instructions on how to get a local instance of FOSSology up and running from source

In the News

The latest announcements, news articles, and events related to FOSSology

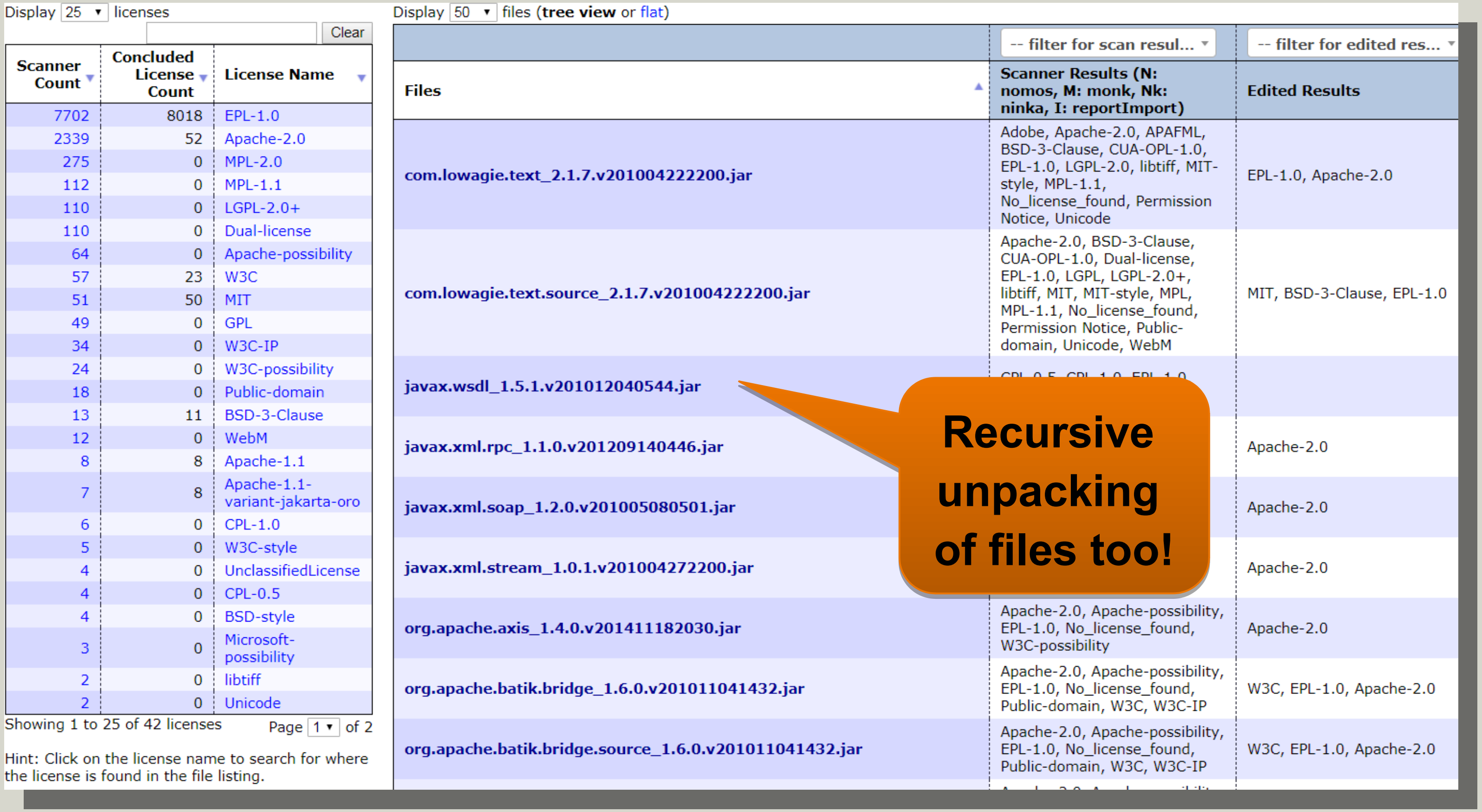
FOSSology is a open source license compliance software system and toolkit. As a toolkit you can run license, copyright and export control scans from the command line. As a system, a database and web ui are provided to give you a compliance workflow. License, copyright and export scanners are tools available to help with your compliance activities.

FOSSology – It is about Overview

SIEMENS

High Level and Drill Down

- Aggregation
  - Folder hierarchy of license findings
  - License-statement oriented view on files
  - Copyright aggregation
- Drill down
  - Navigate into folders
  - Filtering
  - Identify “the single” file



Display 25 ▾ licenses

Clear

Scanner Count	Concluded License Count	License Name
7702	8018	EPL-1.0
2339	52	Apache-2.0
275	0	MPL-2.0
112	0	MPL-1.1
110	0	LGPL-2.0+
110	0	Dual-license
64	0	Apache-possibility
57	23	W3C
51	50	MIT
49	0	GPL
34	0	W3C-IP
24	0	W3C-possibility
18	0	Public-domain
13	11	BSD-3-Clause
12	0	WebM
8	8	Apache-1.1
7	8	Apache-1.1-variant-jakarta-oro
6	0	CPL-1.0
5	0	W3C-style
4	0	UnclassifiedLicense
4	0	CPL-0.5
4	0	BSD-style
3	0	Microsoft-possibility
2	0	libtiff
2	0	Unicode

Showing 1 to 25 of 42 licenses Page 1 ▾ of 2

Hint: Click on the license name to search for where the license is found in the file listing.

Display 50 ▾ files (**tree view** or flat)

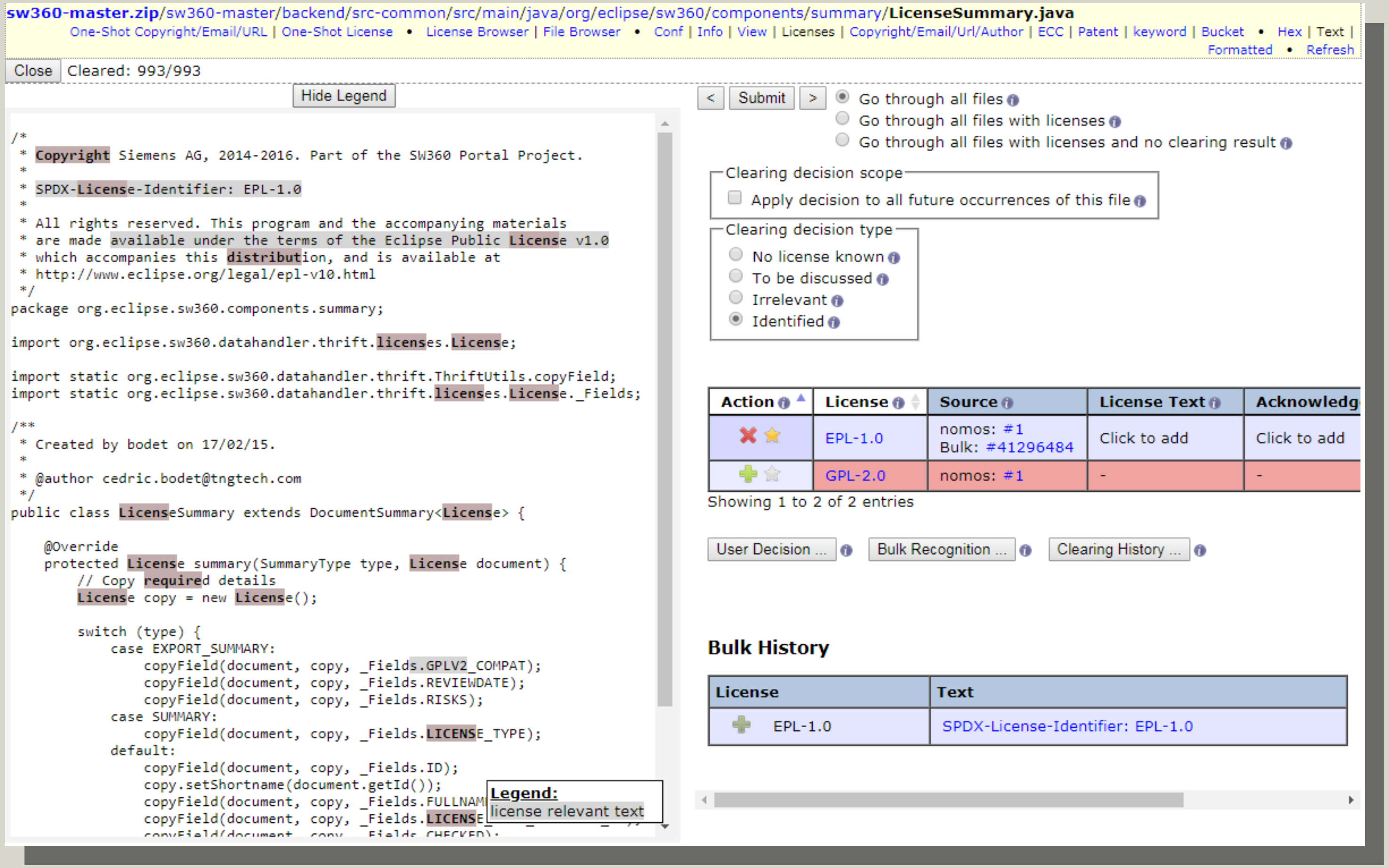
	-- filter for scan resul... ▾	-- filter for edited res... ▾
Files	**Scanner Results (N: nomos, M: monk, Nk: ninka, I: reportImport)**	**Edited Results**
com.lowagie.text_2.1.7.v201004222200.jar	Adobe, Apache-2.0, APAFML, BSD-3-Clause, CUA-OPL-1.0, EPL-1.0, LGPL-2.0, libtiff, MIT-style, MPL-1.1, No_license_found, Permission Notice, Unicode	EPL-1.0, Apache-2.0
com.lowagie.text.source_2.1.7.v201004222200.jar	Apache-2.0, BSD-3-Clause, CUA-OPL-1.0, Dual-license, EPL-1.0, LGPL, LGPL-2.0+, libtiff, MIT, MIT-style, MPL, MPL-1.1, No_license_found, Permission Notice, Public-domain, Unicode, WebM	MIT, BSD-3-Clause, EPL-1.0
javax.wsdl_1.5.1.v201012040544.jar	CPL-0.5, CPL-1.0, EPL-1.0	
javax.xml.rpc_1.1.0.v201209140446.jar		Apache-2.0
javax.xml.soap_1.2.0.v201005080501.jar		Apache-2.0
javax.xml.stream_1.0.1.v201004272200.jar		Apache-2.0
org.apache.axis_1.4.0.v201411182030.jar	Apache-2.0, Apache-possibility, EPL-1.0, No_license_found, W3C-possibility	Apache-2.0
org.apache.batik.bridge_1.6.0.v201011041432.jar	Apache-2.0, Apache-possibility, EPL-1.0, No_license_found, Public-domain, W3C, W3C-IP	W3C, EPL-1.0, Apache-2.0
org.apache.batik.bridge.source_1.6.0.v201011041432.jar	Apache-2.0, Apache-possibility, EPL-1.0, No_license_found, Public-domain, W3C, W3C-IP	W3C, EPL-1.0, Apache-2.0

Recursive unpacking of files too!

FOSSology – Review Findings

Specialized in Review

- Single file review
  - Highlighting of license relevant content
  - Reference text comparison
  - License statement decisions on statement level (“bulk scan”)



sw360-master.zip/sw360-master/backend/src-common/src/main/java/org/eclipse/sw360/components/summary/LicenseSummary.java
One-Shot Copyright/Email/URL | One-Shot License • License Browser | File Browser • Conf | Info | View | Licenses | Copyright/Email/Url/Author | ECC | Patent | keyword | Bucket • Hex | Text | Formatted • Refresh
Close
Hide Legend
<
Submit
>
User Decision ...
Bulk Recognition ...
Clearing History ...

Cleared: 993/993

```
/*
 * Copyright Siemens AG, 2014-2016. Part of the SW360 Portal Project.
 *
 * SPDX-License-Identifier: EPL-1.0
 *
 * All rights reserved. This program and the accompanying materials
 * are made available under the terms of the Eclipse Public License v1.0
 * which accompanies this distribution, and is available at
 * http://www.eclipse.org/legal/epl-v10.html
 */
package org.eclipse.sw360.components.summary;

import org.eclipse.sw360.datahandler.thrift.licenses.License;

import static org.eclipse.sw360.datahandler.thrift.ThriftUtils.copyField;
import static org.eclipse.sw360.datahandler.thrift.licenses.License._Fields;

/**
 * Created by bodet on 17/02/15.
 *
 * @author cedric.bodet@tngtech.com
 */
public class LicenseSummary extends DocumentSummary<License> {

    @Override
    protected License summary(SummaryType type, License document) {
        // Copy required details
        License copy = new License();

        switch (type) {
            case EXPORT_SUMMARY:
                copyField(document, copy, _Fields.GPLV2_COMPAT);
                copyField(document, copy, _Fields.REVIEWDATE);
                copyField(document, copy, _Fields.RISKS);
            case SUMMARY:
                copyField(document, copy, _Fields.LICENSE_TYPE);
            default:
                copyField(document, copy, _Fields.ID);
                copy.setShortname(document.getId());
                copyField(document, copy, _Fields.FULLNAM
                copyField(document, copy, _Fields.LICENSE
                copyField(document, copy, _Fields.CHECKED);
```

Legend:
license relevant text

● Go through all files
○ Go through all files with licenses
○ Go through all files with licenses and no clearing result

Clearing decision scope

□ Apply decision to all future occurrences of this file

Clearing decision type

○ No license known
○ To be discussed
○ Irrelevant
● Identified

Action	License	Source	License Text	Acknowledg
✖ ★	EPL-1.0	nomos: #1 Bulk: #41296484	Click to add	Click to add
✚ ☆	GPL-2.0	nomos: #1	-	-

Showing 1 to 2 of 2 entries

Bulk History

License	Text
✚ EPL-1.0	SPDX-License-Identifier: EPL-1.0

FOSSology SPDX Import and Export

SIEMENS

Import = Consuming SPDX

- Consistency!
  - Handling SPDX conclusions
  - Handling copyright statements
  - Handling new licenses
- Goal was to consistently import the data given existing records

Multiple Use Cases:

- *Checking SPDX from supplier*
- *Correcting existing SPDX and regenerate*
- *Using SPDX of one software package version to generate SPDX for updated version*
- *Transfer conclusions between different FOSSology instances*

FOSSology – Of course you can automate!

REST API

- Manage folders, uploads
- Trigger scans and options
- Download reporting
- More info at: https://www.fossology.org/get-started/basic-rest-api-calls/
- (complete flow explained)

FOSSdriver

- Python based library
- Write your own Python workflow
- Not only what REST API can do
  - … but also manage bulk scans
- More info at: https://github.com/fossology/fossdriver

Command line tools

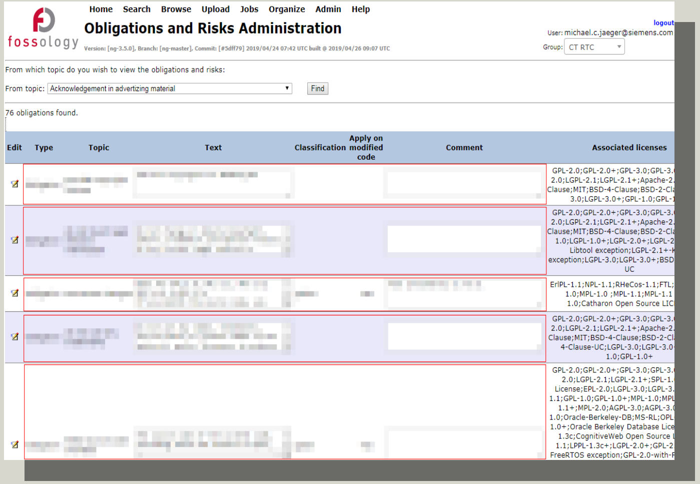
- Many functions and agents have command line interfaces
  - Nomos license scanner
  - Copyright scanner
  - License listings
  - …
- Upload and download tools

FOSSology – License Obligations

SIEMENS

Obligation Mngmt

- Attach obligation entries to licenses
- Admin management UI
- Report documentation for components



Home Search Browse Upload Jobs Organize Admin Help

fossology

Obligations and Risks Administration

Version: [ng-3.5.0], Branch: [ng-master], Commit: [#5dff79] 2019/04/24 07:42 UTC built @ 2019/04/26 09:07 UTC

logout

User: michael.c.jaeger@siemens.com

Group: CT RTC

From which topic do you wish to view the obligations and risks:

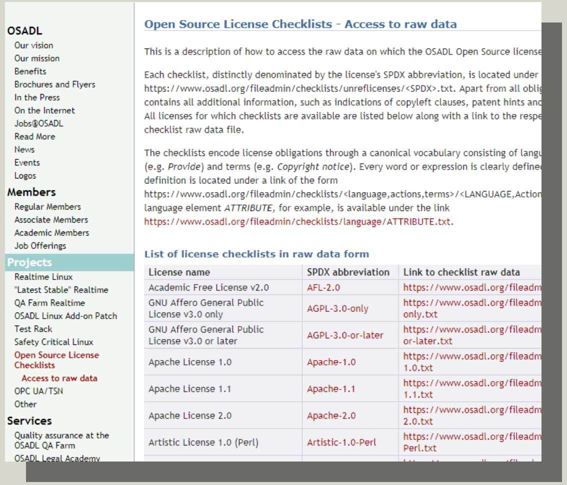
From topic: Acknowledgement in advertizing material Find

76 obligations found.

Edit	Type	Topic	Text	Classification	Apply on modified code	Comment	Associated licenses
✎	[redacted]	[redacted]	[redacted]				GPL-2.0;GPL-2.0+;GPL-3.0;GPL-3. 2.0;LGPL-2.1;LGPL-2.1+;Apache-2. Clause;MIT;BSD-4-Clause;BSD-2-Cla 3.0;LGPL-3.0+;GPL-1.0;GPL-1
✎	[redacted]	[redacted]	[redacted]				GPL-2.0;GPL-2.0+;GPL-3.0;GPL-3. 2.0;LGPL-2.1;LGPL-2.1+;Apache-2. Clause;MIT;BSD-4-Clause;BSD-2-Cla 1.0;LGPL-1.0+;LGPL-2.0+;LGPL-2 Libtool exception;LGPL-2.1+-K exception;LGPL-3.0;LGPL-3.0+;BSD UC
✎	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	ErlPL-1.1;NPL-1.1;RHeCos-1.1;FTL; 1.0;MPL-1.0 ;MPL-1.1;MPL-1.1 1.0;Catharon Open Source LIC
✎	[redacted]	[redacted]	[redacted]				GPL-2.0;GPL-2.0+;GPL-3.0;GPL-3. 2.0;LGPL-2.1;LGPL-2.1+;Apache-2. Clause;MIT;BSD-4-Clause;BSD-2-Cl 4-Clause-UC;LGPL-3.0;LGPL-3.0 1.0;GPL-1.0+
✎	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		GPL-2.0;GPL-2.0+;GPL-3.0;GPL-3. 2.0;LGPL-2.1;LGPL-2.1+;SPL-1. License;EPL-2.0;LGPL-3.0;LGPL-3. 1.1;GPL-1.0;GPL-1.0+;MPL-1.0;MPL 1.1+;MPL-2.0;AGPL-3.0;AGPL-3. 1.0;Oracle-Berkeley-DB;MS-RL;OPL 1.0+;Oracle Berkeley Database Lice 1.3c;CognitiveWeb Open Source L 1.1;LPPL-1.3c+;LGPL-2.0+;GPL-2. FreeRTOS exception;GPL-2.0-with-F

Obligation Source

- Different sources available
  - OSADL License Checklist
  - FINOS OSS Handbook
  - Github: Choose-a-license
- Machine readable formats



OSADL

Our vision
Our mission
Benefits
Brochures and Flyers
In the Press
On the Internet
Jobs@OSADL
Read More
News
Events
Logos

Members

Regular Members
Associate Members
Academic Members
Job Offerings

Projects

Realtime Linux
"Latest Stable" Realtime
QA Farm Realtime
OSADL Linux Add-on Patch
Test Rack
Safety Critical Linux
Open Source License Checklists
Access to raw data
OPC UA/TSN
Other

Services

Quality assurance at the OSADL QA Farm
OSADL Legal Academy

Open Source License Checklists - Access to raw data

This is a description of how to access the raw data on which the OSADL Open Source license

Each checklist, distinctly denominated by the license's SPDX abbreviation, is located under https://www.osadl.org/fileadmin/checklists/unreflicenses/<SPDX>.txt. Apart from all oblig contains all additional information, such as indications of copyleft clauses, patent hints and All licenses for which checklists are available are listed below along with a link to the respe checklist raw data file.

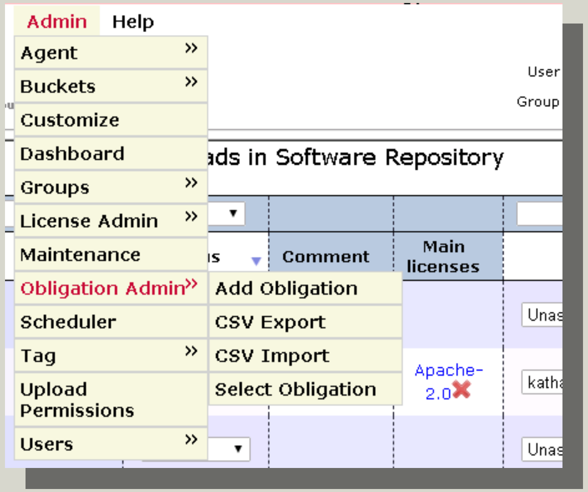
The checklists encode license obligations through a canonical vocabulary consisting of langu (e.g. *Provide*) and terms (e.g. *Copyright notice*). Every word or expression is clearly define definition is located under a link of the form https://www.osadl.org/fileadmin/checklists/<language,actions,terms>/<LANGUAGE,Action language element *ATTRIBUTE*, for example, is available under the link https://www.osadl.org/fileadmin/checklists/language/ATTRIBUTE.txt.

List of license checklists in raw data form

License name	SPDX abbreviation	Link to checklist raw data
Academic Free License v2.0	AFL-2.0	https://www.osadl.org/fileadm
GNU Affero General Public License v3.0 only	AGPL-3.0-only	https://www.osadl.org/fileadm only.txt
GNU Affero General Public License v3.0 or later	AGPL-3.0-or-later	https://www.osadl.org/fileadm or-later.txt
Apache License 1.0	Apache-1.0	https://www.osadl.org/fileadm 1.0.txt
Apache License 1.1	Apache-1.1	https://www.osadl.org/fileadm 1.1.txt
Apache License 2.0	Apache-2.0	https://www.osadl.org/fileadm 2.0.txt
Artistic License 1.0 (Perl)	Artistic-1.0-Perl	https://www.osadl.org/fileadm Perl.txt

Obligation Import

- FOSSology can import records
- Currently: Convert your own data
- Potentially hosted conversion of obligations



© Siemens AG 2019

FOSSology and SW360

Component Analysis Tool

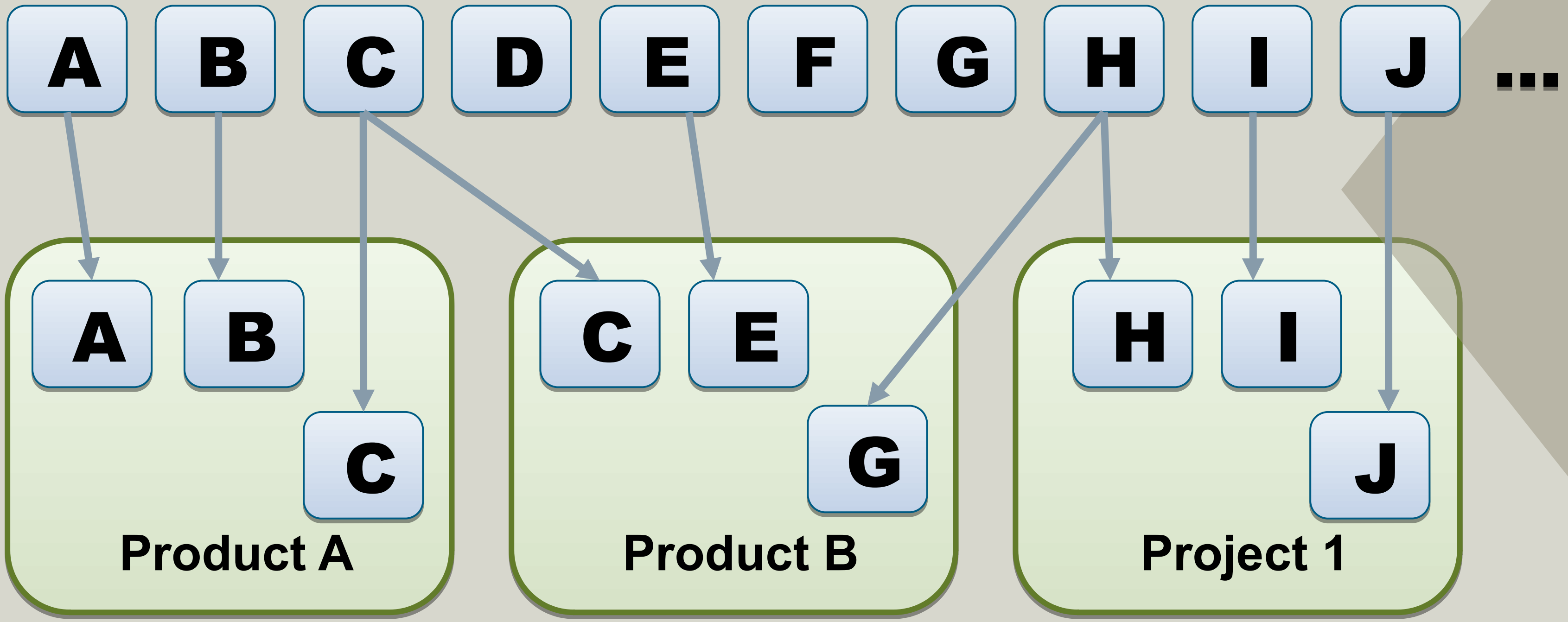
+

Software Catalogue

SW360 Quick Recap

SW360 is a 3rd party software component catalogue

Assigns 3rd party components to products or projects



Inventory (in use)

vs.

Component Library (generally available)

S-BOM-Driven View

SIEMENS

S-BOM: Bill of Material

- Once the software contents are in a number of new use cases:
  - License compliance documentation
  - Collection of source code
  - ECC
  - Vulnerabilities
  - Statistics

SW360 cannot determine the S-BOM, but other OSS tools can:

- *SW360antenna*
- *OSS Review Toolkit*
- *Tern*
- *…*

Compliance Documenation

SIEMENS

Different Use Cases per Product / Project

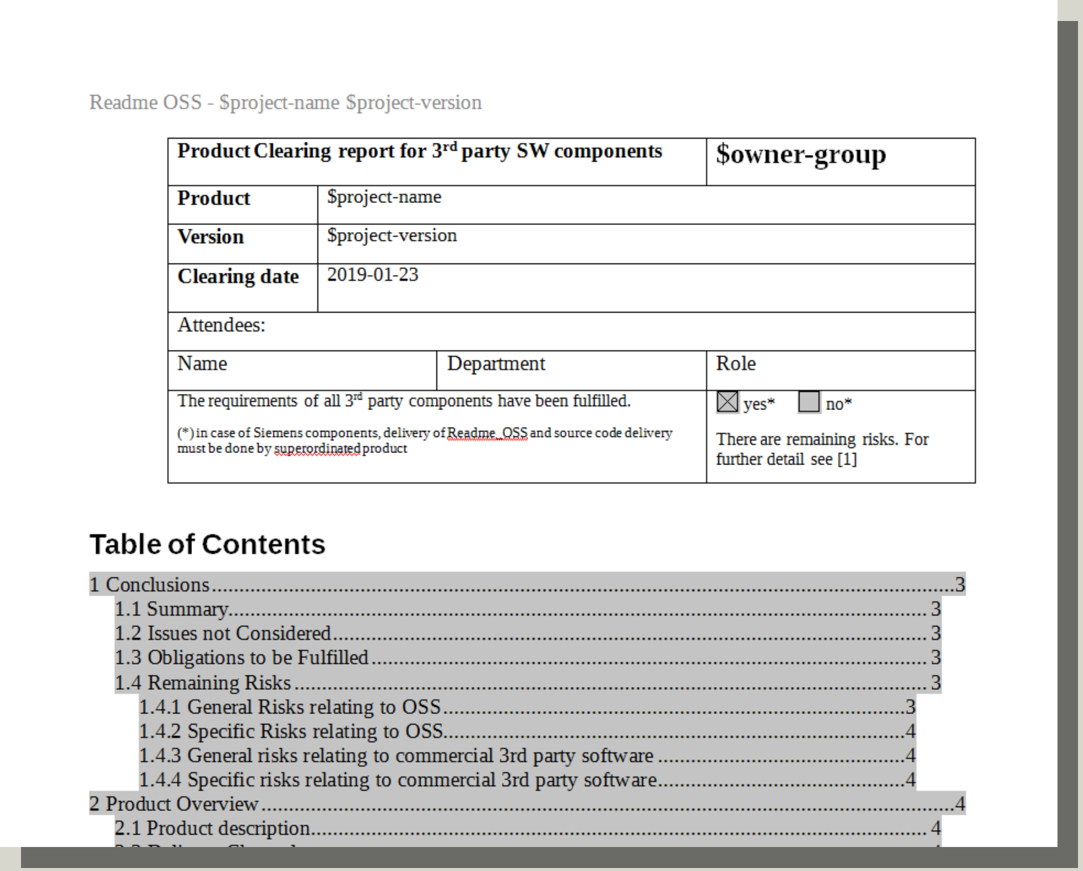
- Component approval
  - Listing approval status of components
- Compliance documentation
  - Generating license texts,
    copyrights from SPDX as HTML or Text
- Source code bundle generation
  - Covering the work of source code collections
- Product approval documentation
  - WIP: Major updates to data model: project obligations

SW360 – Next Feature: Product Approval

SIEMENS

The next use case: Product Approval Document

- Work on product approval document
- Product approval:
  - Do all components fit together?
  - What is the big picture?
  - What is the BOM?
  - What are the total obligations?



Readme OSS - $project-name $project-version

Product Clearing report for 3rd party SW components		**$owner-group**
Product	$project-name	
Version	$project-version	
Clearing date	2019-01-23	
Attendees:		
Name	Department	Role
The requirements of all 3rd party components have been fulfilled. (*) in case of Siemens components, delivery of Readme_OSS and source code delivery must be done by superordinated product		☒ yes* ☐ no* There are remaining risks. For further detail see [1]

Table of Contents

SW360 –Product Approval Documents

SIEMENS

Proposed Document Structure

1 Conclusions

1.1 Summary

1.2 Issues not Considered

1.3 Obligations to be Fulfilled

1.4 Remaining Risks

1.4.1 General Risks relating to OSS

1.4.2 Specific Risks relating to OSS

1.4.3 General risks relating to commercial 3rd party software

1.4.4 Specific risks relating to commercial 3rd party software

2 Product Overview

2.1 Product Description

2.2 Delivery Channels

2.3 Development Details

2.4 Overview 3rd party components/services

3 Obligations

3.1 Common Rules

3.2 Additional Requirements

3.3 Disclosure Document

3.4 Build Instructions

3.5 Source Code Bundle

SW360: REST API

SIEMENS

Integration with other tools

- Check of approved components
- Create S-BOM
- Automated upload of SPDX files to components
- Synchronize component catalogue with other tools

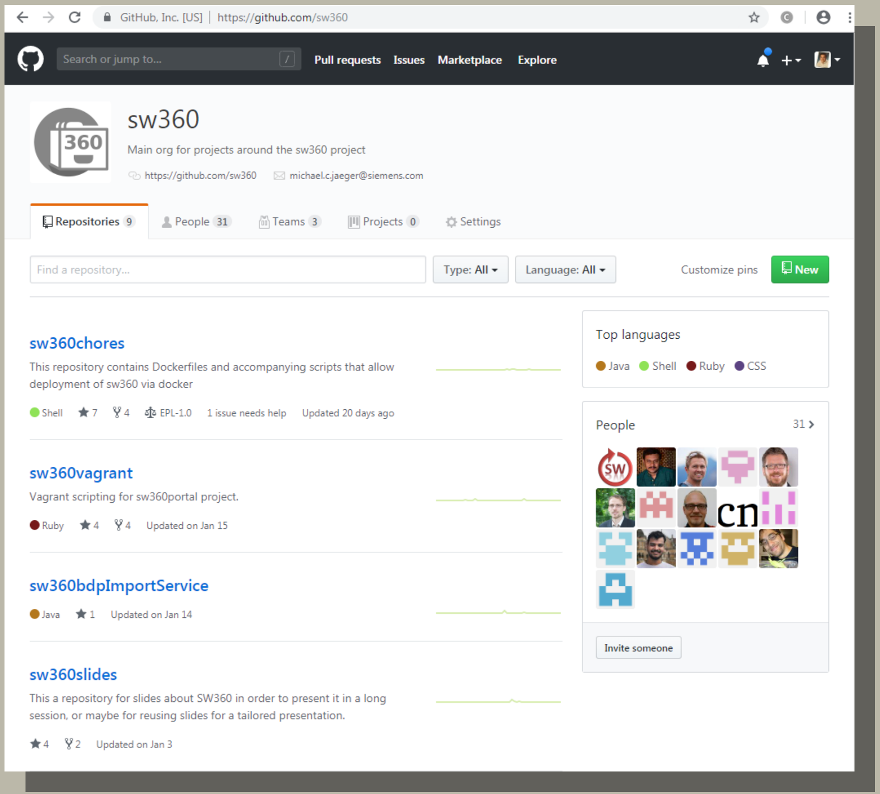
On a normal SW360 instance, full documentation is available:

https://[hostname]:[port]/resource/docs/index.html

SW360: More Projects

SW360 has a number of smaller projects

- **sw360antenna**
  Analyses the build and pulls data from other sources
- **sw360vagrant**
  Full instance deployment, including AWS
- **sw360chores**
  Docker deployment scripts
- **sw360slides**
  Documentation (also in Japanese)



sw360

Main org for projects around the sw360 project

https://github.com/sw360 michael.c.jaeger@siemens.com

Top languages

● Java ● Shell ● Ruby ● CSS

People 31

sw360chores

This repository contains Dockerfiles and accompanying scripts that allow deployment of sw360 via docker

● Shell ★ 7 4 EPL-1.0 1 issue needs help Updated 20 days ago

sw360vagrant

Vagrant scripting for sw360portal project.

● Ruby ★ 4 4 Updated on Jan 15

sw360bdpImportService

● Java ★ 1 Updated on Jan 14

sw360slides

This a repository for slides about SW360 in order to present it in a long session, or maybe for reusing slides for a tailored presentation.

★ 4 2 Updated on Jan 3

https://github.com/sw360

ACT

ACT: Automated Compliance Tooling

Linux Foundation Project

- **Consolidation of efforts**
  Avoiding parallel development
- **Increase interoperability**
  Bring OSS together
- **Helping organizations to manage compliance obligations**
- **More info at:**
  https://www.linuxfoundation.org/press-release/2018/12/the-linux-foundation-to-launch-new-tooling-project-to-improve-open-source-compliance/

Initial Projects

- **FOSSology**
  Scanning, analyzing and reporting
- **TERN**
  Bill of material of containers
- **QMSTR**
  Integration into build systems
- **SPDX Tools**
  Parsing, conversion, verification
-

Thank you for your attention … questions?

Michael C. Jaeger

Siemens AG
Corporate Technology
Otto-Hahn-Ring 6
81379 München

michael.c.jaeger@siemens.com

FOSSology links
https://www.fossology.org/
https://github.com/fossology/fossology

SW360 links
https://sw360.github.io/
https://github.com/sw360/sw360portal