# Step 6 - Review Reports

# Contents

# List of Figures

Return to the Nine Steps Main Page

# Chapter 1

# Introduction

As we reach step six of the Nine Steps for Open Source Governance, it’s a good idea to take a look at everything we’ve already completed:

1. Download, Install, and Configure Sonatype CLM Server
2. Setup Users and Security
3. Create an Organization and Application
4. Import Sonatype Policy
5. Scan an Application

With the previous step, Scan an Application, we now have what we need to take a look at those results. The results themselves are provided in the form of the Sonatype CLM, or Violations, Report. This report will highlight any components that have violated your policies, as well as include additional information representing the overall risk of components used in your application.

In this guide, we’ll provide an overview of the application composition report, as well as offer tips for interpreting results.

# Chapter 2

# Reviewing Evaluation Results

The Application Composition Report provides the results of an evaluation of your application. The results are broken into three key categories:

- Policy Violations
- Security Vulnerabilities
- License Issues.

As mentioned previously, this will be the same report, whether you are using the stand-alone scanner, the CLM Maven plugin, the manual evaluation, or and of the integrated enforcement points (e.g. Sonatype CLM for CI, IDE, Nexus Pro).

Let's take a look at how to access the report first.

**Note**
Depending on the enforcement point, or the stage options you manually selected, your report may be listed under different stages in the *Reporting* area of the Sonatype CLM Server. For example, the default location for the stand alone scanner, is the build stage.

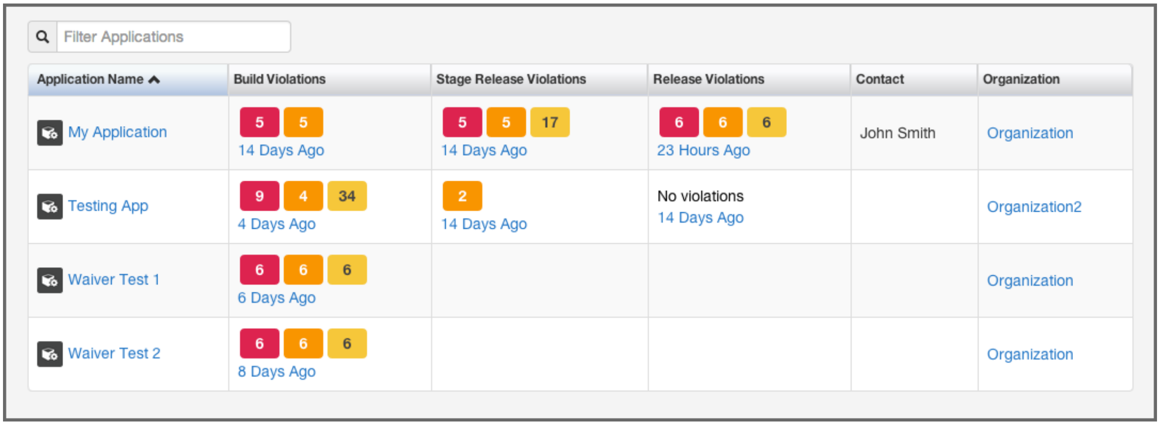
## 2.1 Accessing the Application Composition Report

No matter how the scan was performed, all reports reside on the Sonatype CLM Server and are automatically associated with the corresponding application (via the application identifier). However, there are two distinct ways to access the Application Composition reports.

**Via the Reports Area**

The Reports area, which is displayed by default when you login to the Sonatype CLM Server, can also be accessed by choosing *Reports* from the Global Navigation drop down. These steps outline that process:

1. Log into your Sonatype CLM server with a user account that has proper permissions to view a report for a specific application (at least a member of the developer group for the application would be required).
2. When you are logging in, the *Reporting* area will be displayed. In case you are in a different section of the application, you can always click on the Reporting icon 📈 to return to the Reporting area.
3. You will see two menu items on the left, *Violations* and *Trending*. You want to click on *Violations*, if it is not already selected, to access the violations reports.
4. If you have scanned multiple applications, you will see all of them here. Each application has a separate row with columns for the *Application Name*, links to the Application Composition reports for the different stages (*Build Violations*, *Stage Release Violations* and *Release Violations*), and the contact for the application. The report columns also contain icons with the total counts for *Critical*, *Severe* and *Moderate* policy violations as well as a text indicator for the time the last reports was generated e.g. *2 minutes ago*.
5. Click the the contents in the violations column to access the report.



Filter Applications

| Application Name ▲ | Build Violations | Stage Release Violations | Release Violations | Contact | Organization |
|---|---|---|---|---|---|
| My Application | 5 5<br>14 Days Ago | 5 5 17<br>14 Days Ago | 6 6 6<br>23 Hours Ago | John Smith | Organization |
| Testing App | 9 4 34<br>4 Days Ago | 2<br>14 Days Ago | No violations<br>14 Days Ago | | Organization2 |
| Waiver Test 1 | 6 6 6<br>6 Days Ago | | | | Organization |
| Waiver Test 2 | 6 6 6<br>8 Days Ago | | | | Organization |

Figure 2.1: Reporting Area

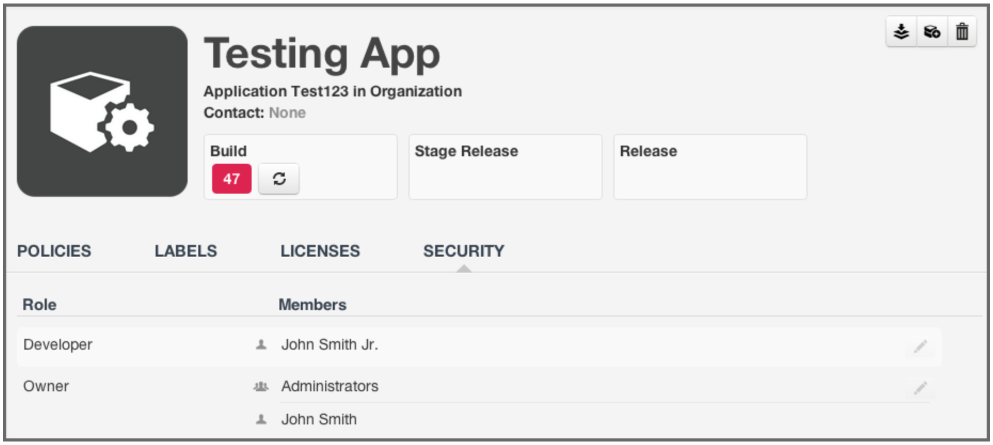
**Tip**
By default this view will be sorted alphabetically by the application name. In addition to the filter, you can also click on the application or organization columns to sort alphabetically ascending/descending.

### Via the Application Area

The Application area is the same place where you can manage policy for your application, reviewing policies unique to the application, as well as those inherited from the organization. Located just below the application identifier and organization, you will see three columns:

- Build
- Stage Release
- Release

These represent the Sonatype CLM stage where the report was generated for/from. For example, if you use the Sonatype CLM stand-alone scanner and don't specify the CLM Stage, it will default to build. When your scan completes and the report is uploaded, it would appear below *Build*. This is highlighted in Figure 2.2.



Application Test123 in Organization
Contact: None

Build: 47

Stage Release

Release

| Role | Members |
|---|---|
| Developer | John Smith Jr. |
| Owner | Administrators<br>John Smith |

Figure 2.2: Application Area

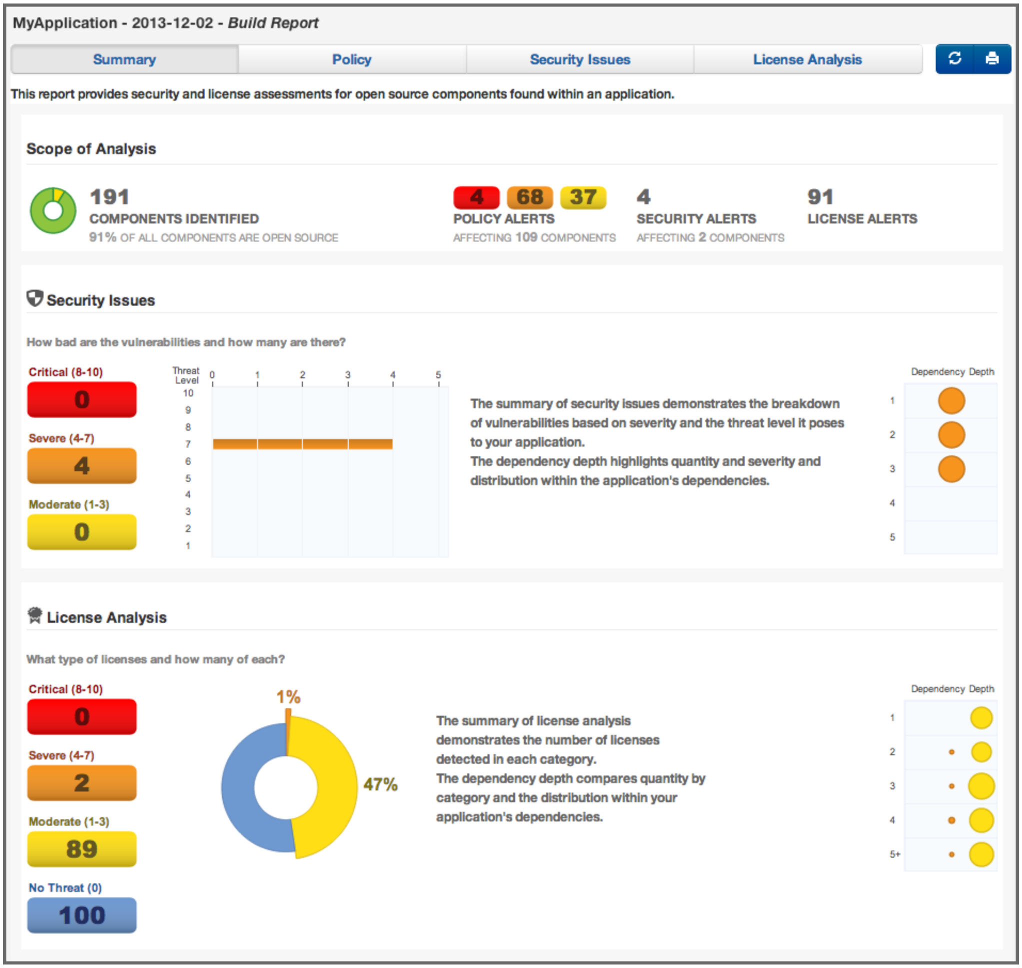
## 2.2 Reviewing the Report

At first glance, you may be surprised at what you see. If you expected an application to have no issues, and now see it has a great deal, don't get upset… yet.

In many cases, a policy can be too stringent or may indicate issues that are not exactly applicable to your application. For example, you may have a security issue that would only affect applications exposed to the public, while your application is for internal use only. Another great example is a license that constrains your code in the event you intend to sell the application.

With that worry out of the way, let's take a look at what's actually in each report.

The *Summary* tab of the report shows a breakdown of what was found. This includes counts for policy violations, security vulnerabilities and license-related issues.



MyApplication - 2013-12-02 - *Build Report*

This report provides security and license assessments for open source components found within an application.

Scope of Analysis

191 COMPONENTS IDENTIFIED
91% OF ALL COMPONENTS ARE OPEN SOURCE

4 68 37 POLICY ALERTS
AFFECTING 109 COMPONENTS

4 SECURITY ALERTS
AFFECTING 2 COMPONENTS

91 LICENSE ALERTS

Security Issues

How bad are the vulnerabilities and how many are there?

Critical (8-10) 0

Severe (4-7) 4

Moderate (1-3) 0

The summary of security issues demonstrates the breakdown of vulnerabilities based on severity and the threat level it poses to your application.
The dependency depth highlights quantity and severity and distribution within the application's dependencies.

License Analysis

What type of licenses and how many of each?

Critical (8-10) 0

Severe (4-7) 2

Moderate (1-3) 89

No Threat (0) 100

The summary of license analysis demonstrates the number of licenses detected in each category.
The dependency depth compares quantity by category and the distribution within your application's dependencies.

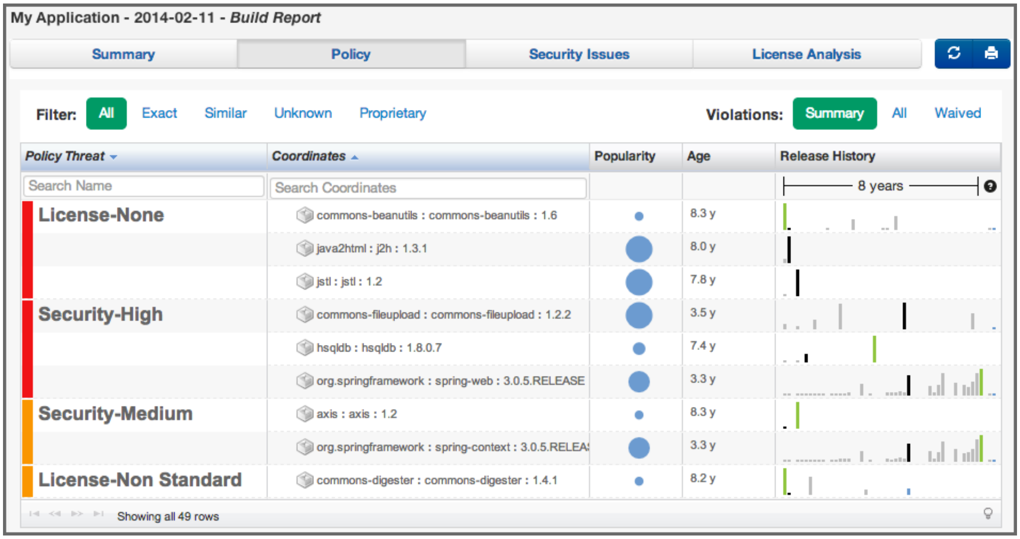
Figure 2.3: Summary Tab of an Application Composition Report

The *Policy* tab provides a list of all components that were found in your application. An example is displayed in Figure 2.4. The list of components is ordered by the level of the threat violation that has been assigned to the policy. In instances where a component has violated multiple policies, only the violation with the highest threat is displayed.

To view the other violations you can use the component information panel (described below), or change what is displayed using the Violations filter on the right. This will allow you to see all violations for your component, though that may result in the appearance of duplicated components.

**Tip**

We have an entire guide dedicated to the various Sonatype CLM Reports.



My Application - 2014-02-11 - *Build Report*

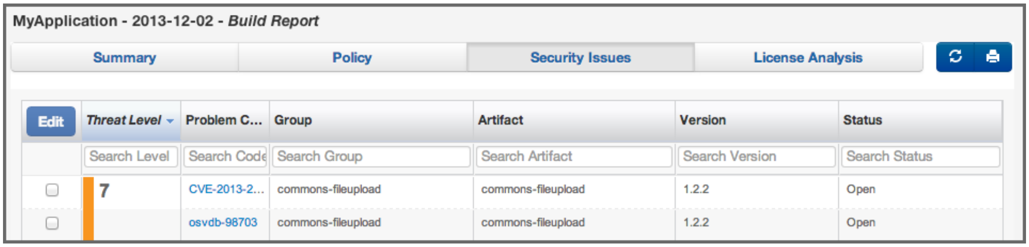
Summary
Policy
Security Issues
License Analysis
Filter: All Exact Similar Unknown Proprietary
Violations: Summary All Waived

| *Policy Threat* | *Coordinates* | Popularity | Age | Release History |
|---|---|---|---|---|
| Search Name | Search Coordinates | | | 8 years |
| License-None | commons-beanutils : commons-beanutils : 1.6 | ● | 8.3 y | |
| | java2html : j2h : 1.3.1 | ● | 8.0 y | |
| | jstl : jstl : 1.2 | ● | 7.8 y | |
| Security-High | commons-fileupload : commons-fileupload : 1.2.2 | ● | 3.5 y | |
| | hsqldb : hsqldb : 1.8.0.7 | ● | 7.4 y | |
| | org.springframework : spring-web : 3.0.5.RELEASE | ● | 3.3 y | |
| Security-Medium | axis : axis : 1.2 | ● | 8.3 y | |
| | org.springframework : spring-context : 3.0.5.RELEA! | ● | 3.3 y | |
| License-Non Standard | commons-digester : commons-digester : 1.4.1 | ● | 8.2 y | |

Showing all 49 rows

Figure 2.4: Policy Tab of an Application Composition Report

The *Security Issues* tab displayed in Figure 2.5 displays all components containing security issues.

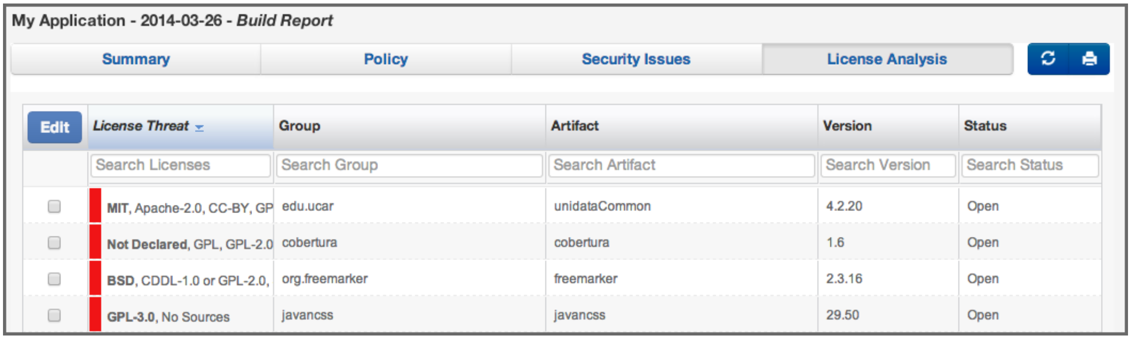


MyApplication - 2013-12-02 - *Build Report*

| Edit | *Threat Level* | Problem C... | Group | Artifact | Version | Status |
|---|---|---|---|---|---|---|
| | Search Level | Search Code | Search Group | Search Artifact | Search Version | Search Status |
| □ | 7 | CVE-2013-2... | commons-fileupload | commons-fileupload | 1.2.2 | Open |
| □ | | osvdb-98703 | commons-fileupload | commons-fileupload | 1.2.2 | Open |

Figure 2.5: Security Issues Tab of an Application Composition Report

The *License Analysis* tab displayed in Figure 2.6 displays all components and the determined details about their license(s).

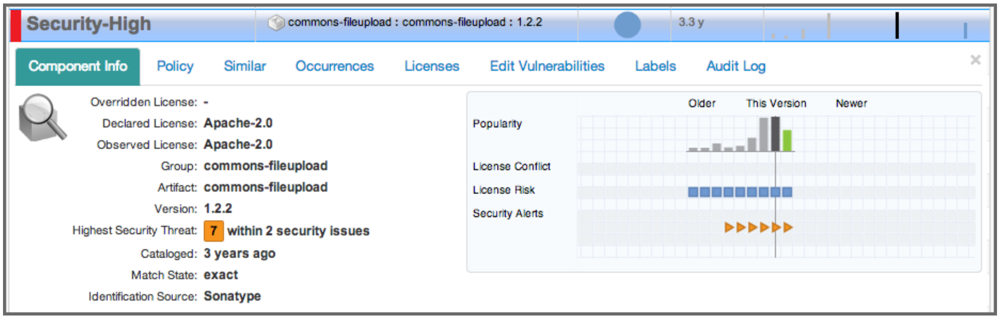


My Application - 2014-03-26 - *Build Report*

| Edit | License Threat | Group | Artifact | Version | Status |
|---|---|---|---|---|---|
| | Search Licenses | Search Group | Search Artifact | Search Version | Search Status |
| □ | **MIT**, Apache-2.0, CC-BY, GP | edu.ucar | unidataCommon | 4.2.20 | Open |
| □ | **Not Declared**, GPL, GPL-2.0 | cobertura | cobertura | 1.6 | Open |
| □ | **BSD**, CDDL-1.0 or GPL-2.0, | org.freemarker | freemarker | 2.3.16 | Open |
| □ | **GPL-3.0**, No Sources | javancss | javancss | 29.50 | Open |

Figure 2.6: License Analysis Tab of an Application Composition Report

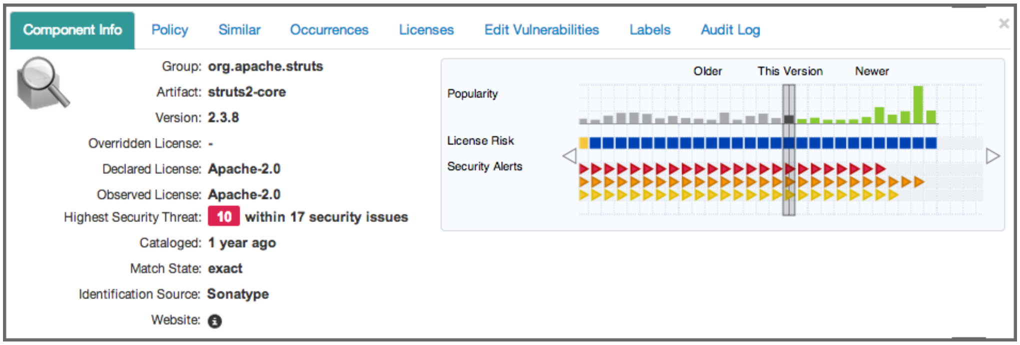
In the *Policy*, the *Security Issues* as well as the *License Analysis* tabs, you can get access to more information about a particular component by clicking on a row in the table representing the component you are interested. The Component Information Panel CIP, with an example displayed in Figure 2.7 shows more specific information about the component.



Overridden License: -
Declared License: **Apache-2.0**
Observed License: **Apache-2.0**
Group: **commons-fileupload**
Artifact: **commons-fileupload**
Version: **1.2.2**
Highest Security Threat: **7** **within 2 security issues**
Cataloged: **3 years ago**
Match State: **exact**
Identification Source: **Sonatype**

Figure 2.7: Component Information Panel CIP for a Specific Component

Clicking on the *Policy* header in the component information panel displays all policy violations for the selected component. As you can see from the example displayed in Figure 2.8 the policies as well as the constraints and the condition values that triggered the policy violation are displayed.



Group: org.apache.struts
Artifact: struts2-core
Version: 2.3.8
Overridden License: -
Declared License: Apache-2.0
Observed License: Apache-2.0
Highest Security Threat: 10 within 17 security issues
Cataloged: 1 year ago
Match State: exact
Identification Source: Sonatype
Website:

Figure 2.8: Policy Tab for a Specific Component Displayed on the Component Information Panel

A number of specifics used in the tabs and the panel are detailed in the following:

**Threat Level**
We briefly mentioned above, that policy violations are organized by threat level. The threat level breakdown is as follows.

- Red / High (10 - 8) - Indicates a component with a severe threat, and should be treated seriously.
- Orange / Medium (7 - 5) - Indicates a component with a moderate threat, and should be treated seriously.'
- Yellow / Low (4 - 2) - Indicates a component with a low threat, and may not pose any serious threat to your application.
- Dark Blue / Informational (1) - Indicates that there is a very low threat, and you should just be aware of a possible issue.
- Light Blue / None (0) - Indicates that no policy has been violated by the component.

**Matching**
It's likely that you started seeing an area that indicates *matching*. As a quick definition, matching employs a series of in-depth algorithms to determine if a component found in your application matches anything known to the Central Repository, or known to the Sonatype CLM Server. That's right, through a claiming process and a proprietary component configuration, you can teach Sonatype CLM to recognize components it may not have otherwise.

**PDF Printing**
The application composition report can be printed to PDF simply by clicking the print icon located in the upper right corner of the report.

**Re-evaluation**
Eventually, when you begin to manage and modify policies, you may simply want to compare the

results from the most recent report with your policy modifications. The re-evaluate button, located to the left of the pdf/print icon will allow you to refresh the results without having to generate a whole new report.

## 2.3 Summary

With the ability to access and review results of your scanned applications, you are well on your way towards true governance of your components. In many ways, you are now nearing the end of the component lifecycle. Remember, even with these results your most important tool will still be communication. Don't be dismayed or persuaded by the results. Go over everything with your teams and work towards your business goals together. For now though, this is what you should take away:

- There are four tabs on a application composition report - *Summary*, *Policy*, *Security Issues* and *License Analysis*.
- You can inspect details about a specific component in the component information panel CIP.
- A report can be created in PDF format to allow printing.
- Refreshing a report can be triggered from the user interface.

# Chapter 3

# Conclusion

Congratulations, you've completed the required steps for Open Source Governance with CLM, the next three steps are completely optional, and depend on your particular purchase. These include:

- Sonatype CLM for CI Installation and Configuration
- Sonatype CLM for IDE Installation and Configuration
- Sonatype Nexus Pro - CLM Edition Installation and Configuration