Sonatype CLM - Release Notes

Contents

List of Figures

Chapter 1

Introduction

The latest version of Sonatype CLM can be downloaded from the Sonatype support site. To view these release notes in a single page format, please download the PDF.

Chapter 2

Upgrade instructions

Depending on your current version of Sonatype CLM, there may be a number of steps required for an upgrade. The best place to start is with our Upgrade Guide.

Chapter 3

Sonatype CLM 1.12

The team has been listening to your feedback, and working to improve how you interact with the Sonatype CLM Server, and the 1.12 release reflects that. We've tweaked and polished, organized and decluttered, added color and changed fonts.

While the UI improvements are the most noticeable, don't let those distract you from a number of additional enhancements to the Sonatype CLM Server as well. Here are the areas that have had improvements in this release:

- Sonatype CLM Dashboard
    - Filter
    - Policy Violations Summary
    - Navigation
    - Overall Performance
- New Policy Violations API
- Application Composition Report
    - License Analysis
    - Security Vulnerability Scoring
- Various Bugs

3.1 Affected Components

The majority of features in this update focus on the Sonatype CLM Server, and will require an upgrade. If you are using any of the following components, you should be sure to upgrade them as well.

- Sonatype CLM CI Plugin
- Sonatype CLM IDE Plugin (Eclipse)
- Sonatype Stand-alone (Command Line) CLM Scanner

3.2 What's New in Sonatype CLM 1.12

Sonatype CLM Dashboard

Outside of the changes to colors and fonts, which improve readability and use, several areas of the dashboard have also been enhanced.

Updated Filter

The filter has been been moved into an expandable and collapsible drawer on the left side of the Dashboard. The filter will also now display which filters are in use, and how many selections have been made. You can read more about using the filter in the Filters section of the Dashboard User Guide.

Policy Violations Summary

A new category, Waivers, has been added. In addition, average age value and the 90th percentile value for age have been added to indicate how long a component has been in a particular category. Read more in the link:../clm-server-dashboard-user-guide/_visual_overview.html[Visual Overview section of the Dashboard User Guide.

Navigation and Overall Performance

The breadcrumb navigation for the Dashboard has been improved such that when clicking on the *Dashboard* breadcrumb will return you to the correct tab within the Dashboard.

In addition to the above, efforts have been made to improve the overall performance of the Dashboard.

New Policy Violations API

We've updated the Sonatype CLM REST APIs to include the ability to retrieve Policy Violation information. For complete instructions on using this API, please read the new Policy Violations section of our API Documentation.

Application Composition Report

Two enhancements have been made to the way License and Security information are displayed. The details have been provided below.

License Analysis

The License Analysis area has been updated so that effective licenses are now displayed. For more information, checkout the License Analysis section of the Application Composition Report Guide

Security Vulnerability

Previously, security vulnerabilities with a level 7 CVSS score were included in the Severe category and indicated with the color orange. These have been moved into the Critical category, which is indicated with the color red. This brings this type of vulnerability into better alignment with the NVD scoring system.

Chapter 4

Special Sonatype CLM for SonarQube Release

In addition to the Sonatype CLM 1.11 (1.11.2) release, Sonatype CLM now supports the SonarQube platform. We are pleased to announce this long-awaited functionality as it will allow you to access summary-level Sonatype CLM information for your applications, as well as link to Sonatype CLM Application Composition Reports, directly from your SonarQube projects.

Sonatype CLM for SonarQube requires Sonatype CLM 1.11 or higher, and can be downloaded from our CLM Downloads KB article. For additional information on installing, configuring and using Sonatype CLM for SonarQube please see our corresponding documentation.

Note
Sonatype CLM for SonarQube requires the Sonatype CLM for Risk and Remediation license. The Sonatype Nexus Pro CLM license does not include this functionality.

Chapter 5

Sonatype CLM 1.11 (Currently 1.11.2)

The most significant improvement in the Sonatype CLM 1.11 release focuses on the development of the new CLM Dashboard. With this, the Dashboard becomes a critical part of your Sonatype CLM Server experience. We'll talk more about that in just a moment, as well as these additional features, all part of the latest Sonatype CLM update.

- Application APIs
- Global Creation
- Component Identification Improvements
- LDAP Performance Improvement
- Various Other Enhancements and Bug Fixes

5.1 Affected Components

The majority of features in this update focus on the Sonatype CLM Server, and will require an upgrade. If you are using any of the following components, you should be sure to upgrade them as well.

- Sonatype CLM CI Plugin

- Sonatype CLM IDE Plugin (Eclipse)
- Sonatype Stand-alone (Command Line) CLM Scanner
- Sonatype CLM Maven Plugin

5.2 Update - Sonatype CLM 1.11.2

This minor update provides a fix for a related security vulnerability, which was identified and fixed.

5.3 Update - Sonatype CLM 1.11.1

This minor update includes enhancements for:

- Sonatype CLM Server updated with new functionality for wildcard usage when searching for users (LDAP or the internal CLM realm). View Documentation
- Sonatype CLM for IDE (Eclipse) added compatibility for m2e 1.5.

5.4 What's New in Sonatype CLM 1.11

Dashboard

After upgrading to Sonatype CLM 1.11, when logging into the Sonatype CLM Server, you will now be taken to the new Sonatype CLM Dashboard (previously the Reports Area was loaded).

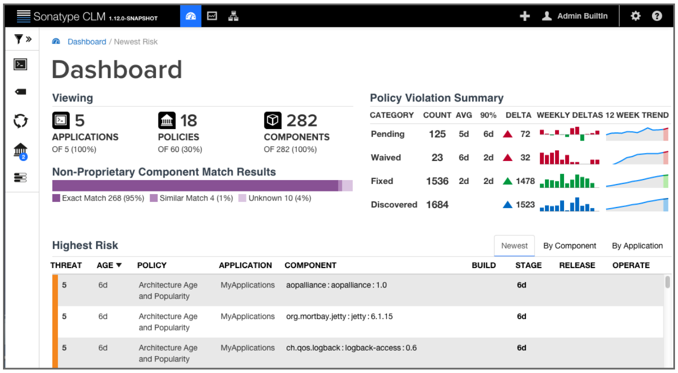
> **Note**
> Users of Sonatype CLM - Nexus Edition will not have access to the new dashboard.

Based on your permissions (assigned roles), you will see aggregated results corresponding to the applications you have evaluated. In addition to a variety of visual information that includes a *View Summary* and a *Violation Summary*, you will also find details related to the newest and highest risk violations a component and an application have incurred.

This data is spread across three main views:

- Newest
- By Component
- By Application

Each of these views can be *filtered* and *sorted* as you desire. This lets you dive even deeper into the data with *new* features like the Component Detail Page which provides up-to-the-moment analysis of your component risk. To learn more about the Dashboard, check out our latest documentation for this area.



Dashboard

Viewing

5	18	282
APPLICATIONS	POLICIES	COMPONENTS
OF 5 (100%)	OF 60 (30%)	OF 282 (100%)

Non-Proprietary Component Match Results

▨ Exact Match 268 (95%) ▨ Similar Match 4 (1%) ▨ Unknown 10 (4%)

Policy Violation Summary

CATEGORY	COUNT	AVG	90%	DELTA	WEEKLY DELTAS	12 WEEK TREND
Pending	125	5d	6d	▲ 72		
Waived	23	6d	2d	▲ 32		
Fixed	1536	2d	2d	▲ 1478		
Discovered	1684			▲ 1523		

Highest Risk

Newest By Component By Application

THREAT	AGE ▼	POLICY	APPLICATION	COMPONENT	BUILD	STAGE	RELEASE	OPERATE
5	6d	Architecture Age and Popularity	MyApplications	aopalliance : aopalliance : 1.0		6d		
5	6d	Architecture Age and Popularity	MyApplications	org.mortbay.jetty : jetty : 6.1.15		6d		
5	6d	Architecture Age and Popularity	MyApplications	ch.qos.logback : logback-access : 0.6		6d		

Figure 5.1: Sonatype CLM Dashboard

Tip

The dashboard introduces a new concept, called risk, which involves a calculation of threat levels for unique policy violations. Be sure to review the guide for a more thorough explanation.

Application REST APIs

A long awaited feature that has been requested many times, is the ability to create and edit application information via API calls. The latest release of Sonatype CLM now supports this ability.

Among the various features of this new public REST API, the most notable are:

- Creating and editing an application
- Setting tags
- Mapping user roles

For detailed instruction on the use of this feature, check out another of our new guides, The API User Guide.

Global Create

One of the most common actions in Sonatype CLM is the creation of new items. This could be applications or organizations, as well as policies, labels, tags, and license threat groups.

No matter the need, the new Global Create functionality allows you to perform these actions from nearly anywhere in Sonatype CLM. Better yet, if you are already in a particular location, the Global Create button will take this into consideration.

For example, if you were looking to create a new application, and were trying to do so from the organization you wish to use, Sonatype CLM will automatically pre-populate this for you.

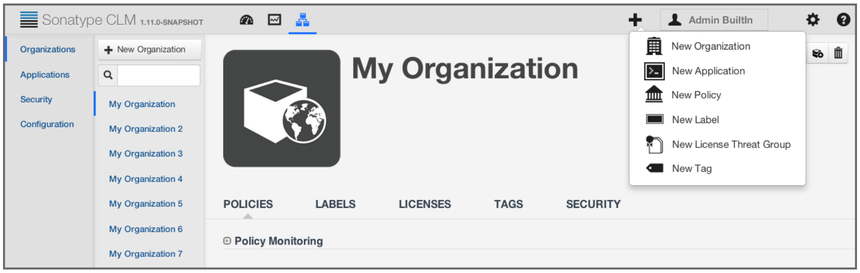


Figure 5.2: Global Create

Component Identification

Two enhancements to component identification have been made:

Claiming Unknown Components

Users have enjoyed the ability to claim components for some time. However, this was previously limited to only those components identified as unknown. Now, users can also claim any component identified as similar, and in these cases, the CIP will remain intact as well. Meaning, you'll see component data that was matched during the evaluation.

Using Regular Expressions in Proprietary Component Configuration

Sonatype CLM will generally treat internally developed components as proprietary. Configuring CLM to identify the proprietary components is an important part of ensuring evaluation results are as accurate as possible. While proprietary component configuration has always been a feature, users can now use regular expressions when specifying them. For more information on this change please review the proprietary components section of the Application Composition Report Guide.

LDAP Performance

In some cases, especially large implementations, using dynamic groups can produce slow LDAP searches within Sonatype CLM. To address this, group searching can now be turned off or on. Making this change will effect how groups can be mapped to roles in Sonatype CLM. For more information, check out our updated LDAP Dynamic Groups and Security Administration documentation.

Additional Improvements

Various updates to maintain consistency in the UI, as well as modification to address any reported bug have been added to this release. In addition two these general updates, two other features have been removed.

- Removed procurement stage option.
- Removed transparent tag color option.

Note
Existing clear tags will be changed to white.

Chapter 6

Sonatype CLM 1.10

The 1.10 release of Sonatype CLM focuses nearly exclusively on enhanced integration with Sonatype's Nexus Professional repository management system. For documentation on all the feature discussed in this update, please read the new Sonatype CLM - Repository Managers User Guide. A number of updates were made to Sonatype CLM systems including:

- Sonatype CLM Server
- Sonatype CLM for Eclipse
- Nexus Professional - Sonatype CLM Edition

6.1 What's New in Sonatype 1.10

Nexus Component Information Panel (CIP)
For users that have purchased a Nexus CLM license, you will now have access to full component information in supported repositories. This includes the ability to see component metadata, the interactive version graph, and the details of any associated policy violations, security vulnerabilities, or license issues.

Project URLs Included in CIP
All areas where the Component Information Panel has been integrated, now include, when available, the URL for the corresponding project. Areas that will display this include:

- Application Composition Report
- Sonatype CLM for Eclipse
- Nexus Professional - CLM Edition

Additional Improvements

- The contact for an application will now be displayed in policy violation emails.
- A number of UI enhancement to improve consistency, look and feel.
- Though not CLM related, Nexus RHC, which uses data similar to CLM, had a number of improvements as well.
- Bug Fixes.

6.2 Upgrading to Sonatype CLM 1.10

Sonatype CLM encompasses several different components including integrations with Eclipse and Hudson/Jenkins. In general the version number of the release refers to the version number of Sonatype CLM Server (currently 1.10), which will always need to be updated to gain access to the latest features.

First, be sure to check our compatibility matrix, Knowledge Base article. Next, if you are using a version of the Sonatype CLM Server prior to version 1.9, please follow these specific instructions:

Chapter 7

Sonatype CLM 1.9.1

The 1.9.1 release of Sonatype CLM extends the capabilities of the Maven plugin and provides a minor update to the PDF version of the Application Composition Report. These updates affect the following CLM Components:

- Sonatype CLM Server
- Sonatype CLM Maven Plugin

7.1 What's New in Sonatype CLM 1.9.1

This release provides improvements in two areas:

Sonatype CLM Maven Plugin
The plugin will now allow users to export basic information about the application evaluation into a JSON file. This file includes URLs to the results of the report. In addition, we have provided a REST API for this functionality. Details for using this API can be reviewed at our Sonatype CLM REST API Knowledge Base. If this functionality seems familiar, that's likely because it was added as part of the Stand-alone scanner update in the 1.9 release of Sonatype CLM.

PDF version of the Application Composition Report

The report has been modified to now include the contact for the application, which is managed via the Application area on the Sonatype CLM Server.

Note

The version of the Sonatype CLM Maven plugin (2.2.0) is different from the overall Sonatype CLM version (1.9). All version information is provided as part of the compatibility matrix

Chapter 8

Sonatype CLM 1.9

The 1.9 release of Sonatype CLM introduces a wide range of expanded functionality that encourages improved categorization of your applications, as well as a number of new features aimed at helping you fine-tune your policies.

The features and improvements for this release affect the following CLM components:

- Sonatype CLM Server
- Sonatype CLM Stand-alone Scanner

Note
Depending on what components your company has purchased and/or uses, you will want to make sure you update your entire Sonatype CLM Suite.

8.1 What's New in Sonatype CLM 1.9

At the core of this release is the introduction of Tags. Tags provide a way to identify specific characteristics that applications share, and direct policies to be matched to applications with those tags.

We'll discuss tags in more detail in the next section. However, in addition to tags, this release also includes improvements to:

- Waivers - entire policies can now be waived. This can range from waiving a single component, to waiving all components for all applications.
- Reporting Area - the Reporting Area dashboard now includes the organization, allowing you to search for, and sort by, organizations.
- Various UI Improvements - among a number of small tweaks and improvements, you can now identify your specific version of Sonatype CLM.
- Stand-alone Scanner - users can now specify a location for a JSON file, which includes information about the completed scan, and a URL to the Application Composition report.
- Application Composition Report - The report has been updated to provide a number of new views on the policy tab, including specific icons and views for identifying components that have been waived.
- Security vulnerability identified and fixed.
- Various small bug fixes.
- All documentation has been updated to reflect all new features. Documentation can be accessed via the help area in Sonatype CLM, or in our Sonatype CLM Documentation area on our website.

8.2 More About Tags

As we mentioned, tags provide a way to identify common characteristics (e.g. distributed) for applications in your organizations. Tags are created at the organization level, and then be applied to individual applications. Not all applications will (or should) have the same tags, which is where the next element of tags, gives you even more flexibility in fine-tuning your policies and policy management processes.

Policies now have an additional option which allows you to select certain applications based on their tags. If an application has applied this tag, it will be evaluated against that policy. Now, you have an easy way to establish both more relaxed, as well as more stringent policies, depending on the risk or level of quality associated with the application.

There's even more to tags than policies and applications though, this latest feature also includes:

- Tag Colors - In addition to custom tag names and descriptions, the color of each tag can also be selected.
- Tag Import - When importing sample policies, tags will also be included.

Chapter 9

Sonatype CLM 1.8

The information provided below represents the updates provided with Sonatype CLM 1.8 release. All improvements listed here, are also part of the latest release.

9.1 What's New in Sonatype CLM 1.8

All of the features described below are part of the Sonatype CLM 1.8 release. In addition to what is described here, all documentation has been updated and is available by clicking the new Online Help link in the Help Menu of the CLM Server. Additionally, you can access Sonatype CLM documentation via the Sonatype CLM Documentation Index.

Continuous Policy Monitoring

Policy Monitoring provides a way to continuously review an application, and then be alerted if new violations have occurred Don't worry though, you don't have to do this for every policy. Meaning, you won't need to be woken up in the middle of the night just because one of your components is now too old. However, if one of your components has a critical violation, you'll have that information ready to make a decision.

Simplified Application Upload and Evaluation

The CLI, or Stand-alone Scanner, has been providing users with a way to quickly and effectively evaluate applications on the fly. Now, you have that same functionality right within the CLM Server interface. All you need to do is select a file to evaluate, pick the application the evaluation is for, and then decide which CLM Stage it should represent. Better yet, if you're evaluating a really large application, you don't need to wait for the evaluation to complete before returning to other tasks in CLM.

Generic CI Support

Currently Sonatype CLM integrates seamlessly with the Hudson and Jenkins CI servers. However, we realize there are alternatives available, and have updated the CLI/Stand-alone scanner to support integration with other continuous integration servers. The main improvements include an update to exit codes that provide the ability to warn or fail builds when a policy is evaluated, as well as the ability to allow the chosen build system to ignore any exit codes. This means you can potentially integrate any build system directly into your CLM process without worry of significant impact to your current process.

General Enhancements

A number of improvements have been made to the way users interact with Sonatype CLM from policies to the existing reports. This includes:

- When using the CLI/Stand-alone Scanner, you can now customize the CLM Stage the evaluation will apply to.
- Applications now have a field for setting the contact.
- A link to online help is now provided as part of the new Help menu.
- Various bug fixes, and data updates.

Chapter 10

Sonatype CLM 1.7

The information provided below represents the updates provide with the 1.7 release. All improvements listed here, are also part of the latest release.

Important
One of the key enhancements related to this release is the addition of Security Administration (User Accounts and Roles). For those upgrading from a previous version, please see specific instructions below.

10.1 Update to Config.yml

One of the most requested features found in version 1.7 of the Sonatype CLM Suite, is Security Administration. Going forward, Sonatype CLM no longer allows anonymous access in Sonatype CLM for IDE. In addition, access to reports directly in the Sonatype CLM for CI interface is no available. To provide a more secure environment, these reports are now exclusive to the Sonatype CLM Server, and will require a user name and password to login. However, a link to these reports is still provided within the native Hudson and Jenkins environment.

If you are upgrading from a previous version, you will need to add a specific line to your current config file, under the *loggers:* area.

Line to Add

```
"org.apache.shiro.web.filter.authc.BasicHttpAuthenticationFilter": INFO
```

After adding, your config should look like this:

```
loggers:
    "eu.medsea.mimeutil.MimeUtil2": INFO
    "org.apache.http": INFO
    "org.eclipse.jetty": INFO
    "org.apache.shiro.web.filter.authc.BasicHttpAuthenticationFilter":  ↩
        INFO
```

Warning
Failure to add this line to your **config.yml** file will result in credentials being published to the Sonatype CLM log file and is considered insecure.

10.2 Invalid Email Address

One of the available actions for Sonatype CLM is the ability to send an email with the most recent results of the application composition report. However, in some cases an invalid email resulted in an error. Sonatype CLM will now check for a valid email address, and if an invalid email is found, the policy will not be evaluated, and an error will be generated. The errors will be displayed in the logs of the CLM Server.

To address the error, simply correct the email address that is indicated as invalid.

10.3 What's New in Sonatype CLM 1.7

Security Administration
In previous versions of Sonatype CLM, all access was anonymous. That is, anyone with access to the Sonatype CLM server, or the add-ons for various enforcement points (e.g. Sonatype CLM for

CI and IDE), would have full access to all Sonatype CLM functionality. This is no longer the case with the latest version of Sonatype CLM.

However, this isn't merely the addition of user names and passwords, administrators and managers now have access to a wide range of security features. This includes:

- Internal (CLM) Realm Support
- Support for LDAP (including users and groups)
- Separate roles for developers, organization owners, and administrators
- Required authentication from Sonatype CLM for IDE
- Required authentication when viewing reports from Sonatype CLM for CI

Tip
When configuring LDAP, static groups are preferred over dynamic ones, and will generally perform better if you have a large number of LDAP users.

For a full walkthrough of all Security Administration, and guidance in setting up these features, please review our Security Administration Guide.

New Trending Report

Reviewing violation results via the Application Composition Report is at the heart of ensuring your policies produce violations that match the goals of your business. However, understanding how things are shaping up over time has been more of a manual process.

The New Trending Report changes this. Now, you can see the progress you are making in reducing your usage of components that introduce risk into your organization. This report will look over results from the last twenty days, and then provides a summary of your policy violations and components.

There's a lot more to this report though, read all about it in the Trending Report section of our Reports-Guide.

Policy Import

While the ability to import policies has been a supported function for some time, the process was manual, and in many regards cumbersome. This has now been completely updated and has user interface updates to make things even easier.

If you are looking to import policy into an organization or application, our new Policy Management guide has everything you need.

Component Search

For many users, most in fact, a component exists in multiple applications. However, understanding which applications that component is in, is not provided by reviewing a single report. To address this, users now have access to this information. All you need an API request through a service such as Curl, and you can send a query for identifying which applications contain a specific component.

For more on this feature, review our Knowledge Base article, How can I see in which applications a component is found?

General Enhancements

A number of improvements have been made to the way users interact with Sonatype CLM from policies to the existing reports. This includes:

- Label description and color is now provided during policy creation.
- Policy Violations are now included as part of the Application Composition Report PDF.
- Claimed components can now have their license information manually overridden.
- GAV coordinates are now included as part of the Nexus RHC data.
- Various bug fixes, and data updates.

Documentation Update

As you've seen throughout these notes, a number of new guides have been created. We encourage you to review all of our documentation for Sonatype CLM. Head there now, and let us know what you think.