

Why You Should Care About Open Source Licensing

You can build better software faster with Open Source Software (OSS) components. But you must ensure that your organization meets component-licensing terms. Violating the terms of an open source license is copyright or intellectual property infringement and can lead to legal and financial penalties.

WHAT IS OPEN SOURCE LICENSING?

Source-code authors own their work and it is protected by copyright. Open source licensing protects the intellectual property rights of the original creators and determines the way in which it may be used and distributed by others.

COMMON OPEN SOURCE LICENSE TYPES

There are hundreds of open source licenses, each with distinct rules and regulations regarding the licensing of OSS components. The most common types of open source licenses are:

- **“Permissive”** licenses, such as Apache, MIT or BSD, allow you to copy, modify and distribute derivative works with limited conditions. These typically include attribution to the original authors and a copyright notice. These licenses most often are found on lower-level projects.
- **“Weakly Protective”** licenses, such as Mozilla, Eclipse and the GNU Lesser General Public License (LGPL), allow you to copy, modify and distribute larger works that include open source components, but require you to make source code and documentation available for any modifications to the initial component itself. These licenses tend to be used in libraries or platforms.
- **“Strong Copyleft”** licenses, like the GNU General Public License (GPL), require you to license applications under the same Strong Copyleft license even if they just include a single component licensed in this way (see Figure 1). This includes the requirement that the application’s source code be made available when it is distributed outside of your organization. In some cases, such as the Affero General Public License (AGPL), the right to obtain source code is extended to any network user of the licensed work. This type of license is generally incompatible with commercial software.

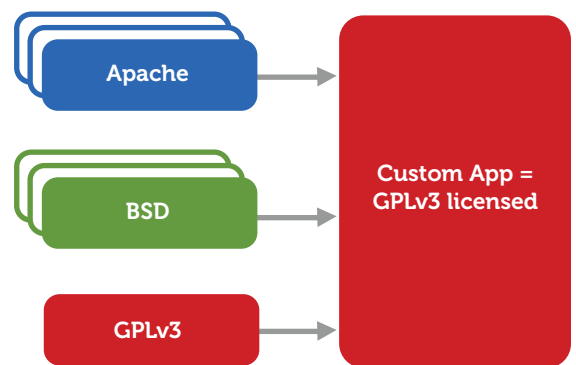
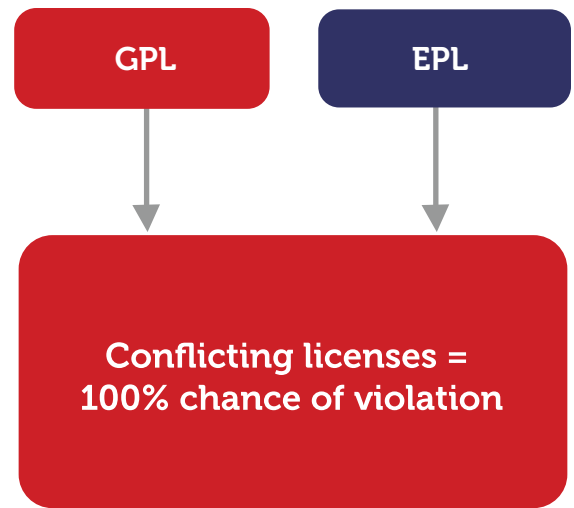


Figure 1. Using a Copyleft licensed (e.g., GPLv3) component requires the application to be licensed under that same Copyleft license.

Choosing the right license type for a new application and adhering to all open source license obligations throughout the software development lifecycle can be tricky. Several common license types are incompatible and cannot be combined into a new application (see Figure 2). You'll need the right tools and information to select appropriately licensed components – and ensure that you are complying with license terms.



JAVA OPEN SOURCE DEPENDENCIES

Java component-based development introduces unique licensing issues:

- It is often difficult to determine a component's licensing terms. Project owners may omit licensing information or submit incorrect information when publishing their project to distribution sites such as the Central Repository.
- You must consider the license of every component, including all dependencies. If even a single Copyleft licensed component, no matter how many levels deep, is included in your application, then the entire application must be licensed under that Copyleft license (see Figure 3).

Figure 2. You can't combine components with incompatible licenses into an application.

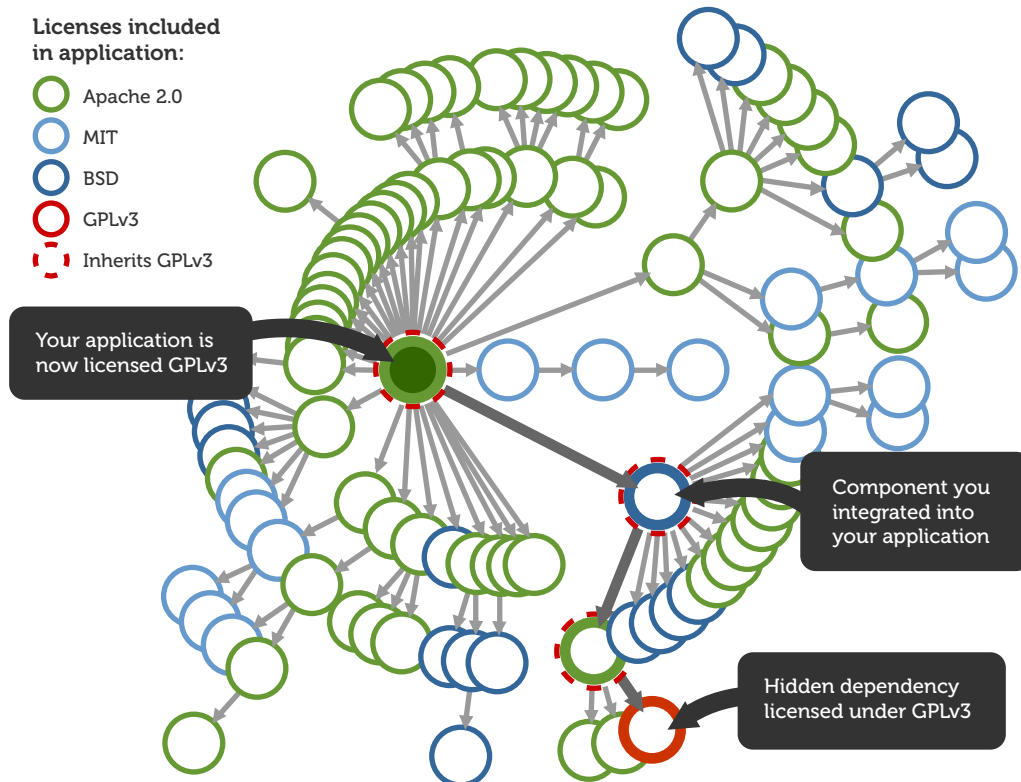


Figure 3. Transitive dependencies greatly increase the complexity of license management. You need to meet the obligations of every component used by your applications, not just those directly integrated.

CUT THROUGH THE COMPLEXITY

Evaluating the legal obligations of open source components can be difficult and time-consuming. Sonatype Insight can help. Insight delivers actionable quality, security, and licensing information about open source components utilized throughout your organization. By integrating with your existing tools and processes it gives you the licensing information and management you need, when and where you need it:

- Enable developers to choose appropriately licensed components during design and development with information in their IDE
- Identify and manage component licensing during the build phase to address issues quickly and avoid costly rework
- Scan your existing applications to identify problematic licenses, including all dependencies.
- Gain visibility into which licenses are being downloaded by your organization from the Central Repository.

Learn more at www.sonatype.com/Insight