

Why should you care about open-source licenses

Oleksii Borysenko

Developer Advocate, Code Exchange Lead, Cisco

At Cisco, I have been developing and maintain platform for code exchange. Code Exchange <https://developer.cisco.com/codeexchange/> is an aggregator of open-source projects.

The session includes the following items:

- Choose the license for your project from scratch
- Which license should choose for easy use project as part of proprietary software
- Multi-licensing
- How to manage the project with different licenses
- Compatibility of licenses
- Organize licensing if the project contains forks of other projects or uses project code with different licenses
- Tools for managing open-source license

Disclaimer:

- Information in this session should not be considered legal advice.

Intro

Developers do not often pay attention to licenses when using various open-source projects. We can often use projects/part of a project or functions for our applications and programs without thinking about how it might affect the future. Do you need to keep the copyright? What are requirements and obligations of different licenses? In this session, I want to highlight the issue of choosing licenses for the project and the specs of using projects with different types of licenses.

Open-source license

A license for open-source projects is a legal contract that regulates the relationship between one or more authors and the user. It includes the following information:

- Description of the terms of use of the project or code, including usage in commercial programs.
- Definition of what can and cannot be done with the software components, the obligations, and the features of usage.
- Regulation of the responsibility of the authors and contributors to the project.

Open-source license

So, if you start from the end, we have ready-for-use projects or proprietary software that uses open-source licenses. But you check the license and find license issues, license conflicts, or use projects without a license.

What problem can effect this?

- You need to replace and to redevelop a part of the source code
- Negative press coverage for non-compliance
- Loss of reputation with open-source community and customers
- Change the license of your derived work
- Be able to disclosure corresponding source codes by request

The following diagram shows statistics data for the licenses that are used on the Cisco Exchange platform. The data includes published use cases as of August 2022.

License	%
Other+Cisco Sample Code license	32.46
MIT	25.81
Apache-2.0	16.94
BSD3-Clause	14.96
GPLv3	8.16
BSD2-Clause	0.63
MPL2.0	0.32
AGPLv3	0.24
GPLv2	0.16
LGPLv3	0.08
LGPLv2.1	0.08
EPL-1.0	0.08
Artistic-2.0	0.08

Licenses can be divided into:

- Copyleft (GPL, Mozilla Public License, Eclipse, CC-SA, Microsoft Public License, etc.),
- Permissive (Apache, MIT, BSD, etc.).

Copyleft can also be divided into “weak” and “strong”:

- "strong" include GNU, GNU Affero General Public License.
- "weak" — for example, Eclipse, GNU Lesser General Public License (LGPL).

License text

Most open-source licenses contain specific obligations concerning information and documentation. For example, many licenses require that the respective license text to be delivered with the software when it is distributed.

Cisco AnyConnect Secure Mobility Client

Version 4.10.05111



Copyright (c) 2004 - 2022 Cisco Systems, Inc. All Rights Reserved.
Cisco, the Cisco Logo, Cisco AnyConnect, AnyConnect and the AnyConnect logo are registered trademarks or trademarks of Cisco and/or its affiliates in the United States and certain other countries.

Installed Modules:

VPN, System Scan, Roaming Security, Network Visibility, Customer Experience Feedback

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit:

<https://www.openssl.org>

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

This product includes software written by Tim Hudson (tjh@cryptsoft.com)

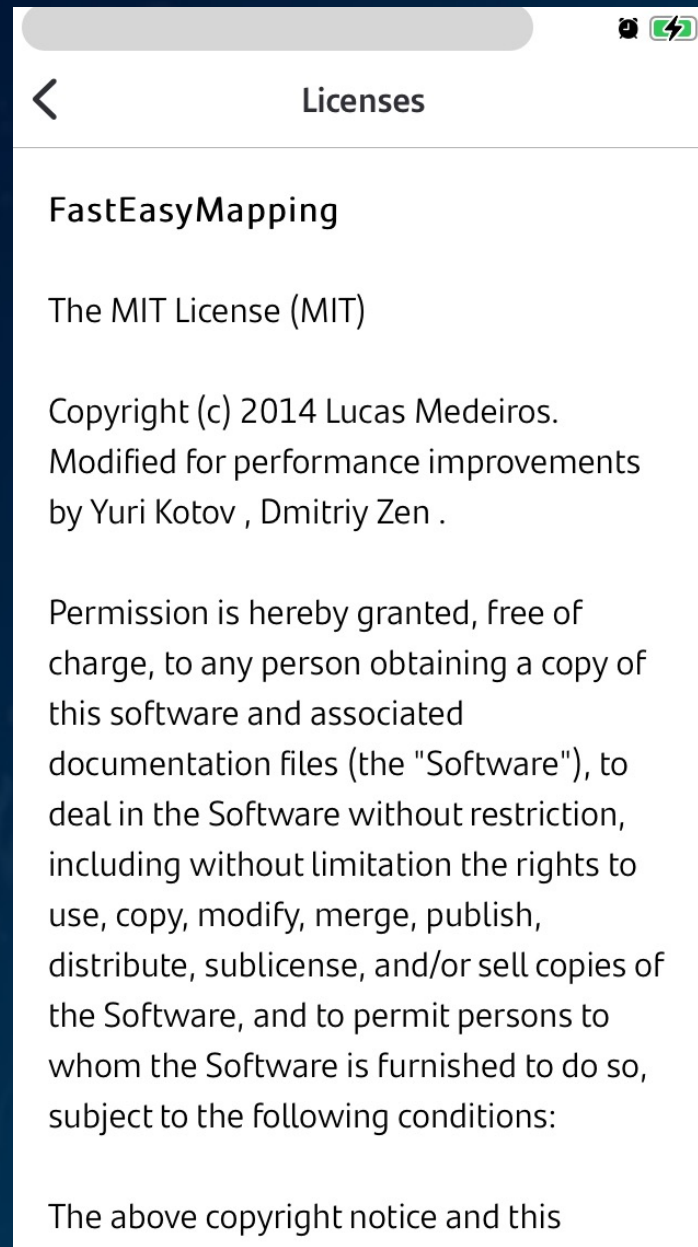
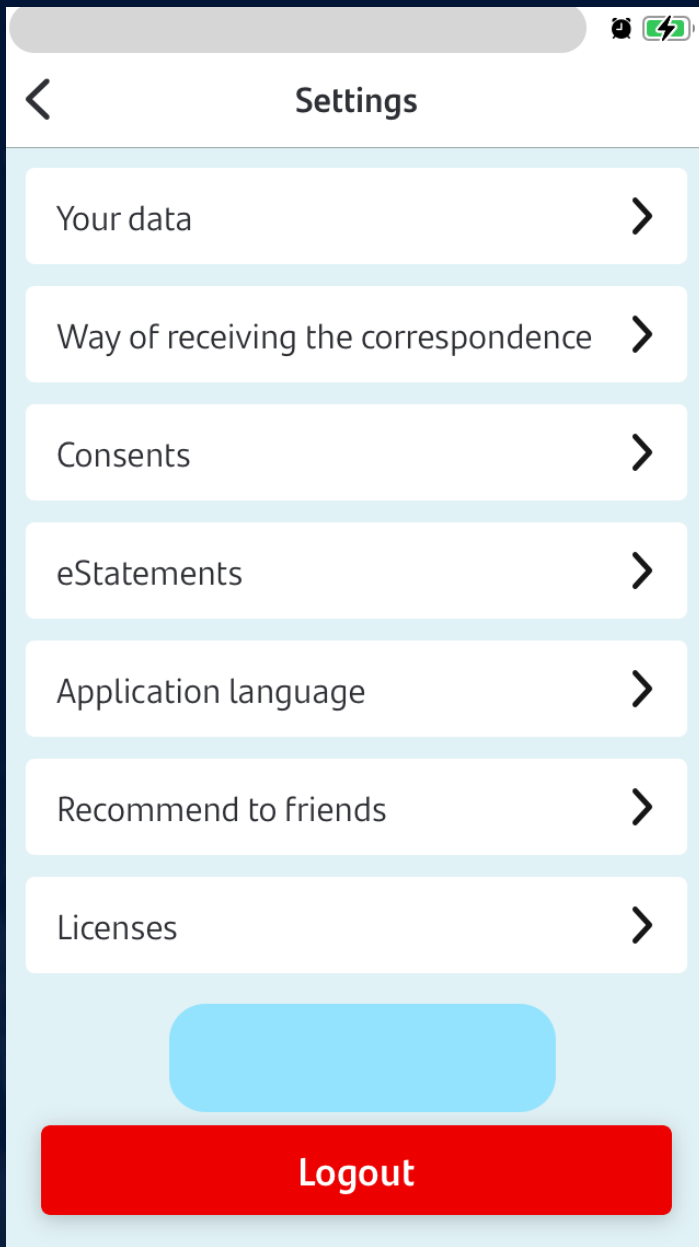
This product incorporates the libcurl HTTP library:

Copyright (c) 1996 - 2019, Daniel Stenberg, (daniel@haxx.se).

[End User License Agreement](#)

[Cisco Online Privacy Statement and the AnyConnect Supplement](#)





Let's consider popular open-source license

GNU General Public License

The GPL is generally considered an "aggressive" license, which sometimes is incompatible with other copyleft licenses.

In addition, this license is often called a viral license because it is transferred from project to project.

If you use GPL-licensed projects in your software, then all your software is considered a "work based on" the GPL. Copyright and patent usage rights are unregulated. Who then monitors that GPL projects remain copyleft? Various associations and unions do this, but in addition, individual contributors and free software evangelists (Harald Welte) also act as plaintiffs in cases of violation of the license agreement. Besides Free Software Foundation (FSF) — this organization owns the rights to parts of the GNU systems project.

GNU General Public License

Exceptions to the GNU Lesser General Public License

Until 1999, the license was called the GNU Library General Public License. GNU LGPL was created not to violate the principles of free software, so that developers can use this license for their libraries and scripts. In addition, other developers and companies can use the relevant projects with the LGPL license without effecting the license of the main/compiled project or derivative work (including commercial ones).

Projects using the GNU GPL include:

Linux Kernel

WordPress (GNU GPL-2.0)

Solidity The Smart Contract Programming Language (GNU GPL v3.0)

Grafana (GNU Affero General Public License v3.0)

Signal (GNU Affero General Public License v3.0)

Apache 2.0

Unlike other permissive licenses, it has clause 3 (3. Grant of Patent License.), which refers to patents. The Clause governs the disposal of patents: participants grant permission to use any of their patents that may relate to their contribution.

The popularity of this license is constantly growing, not least because this type of license has been chosen as mandatory for projects by the Cloud Native Computing Foundation.

MIT

The license allows you to do whatever you want to with the code; the only requirement is keeping the original license and attribution information. If choosing among permissive licenses for your project, I will choose and recommend MIT.

In a nutshell, it is straightforward, does not require additional NOTICE files, and you can use copyrights of any organization and trademark.

Projects using MIT: Visual Studio Code, Julia Language, Electron, Angular.js, Rails

Automatically apply the specific license

There are projects and resources that automatically apply the specific license to code/content that you created by using the related project.

For example:

The ISC License is the default license used when setting up a new NPM package with the `npm init` command.

The ISC License (ISC) is functionally identical to the MIT License, but with some wording seemed unnecessary removed.

CodePens are automatically MIT licensed.

Projects without a license

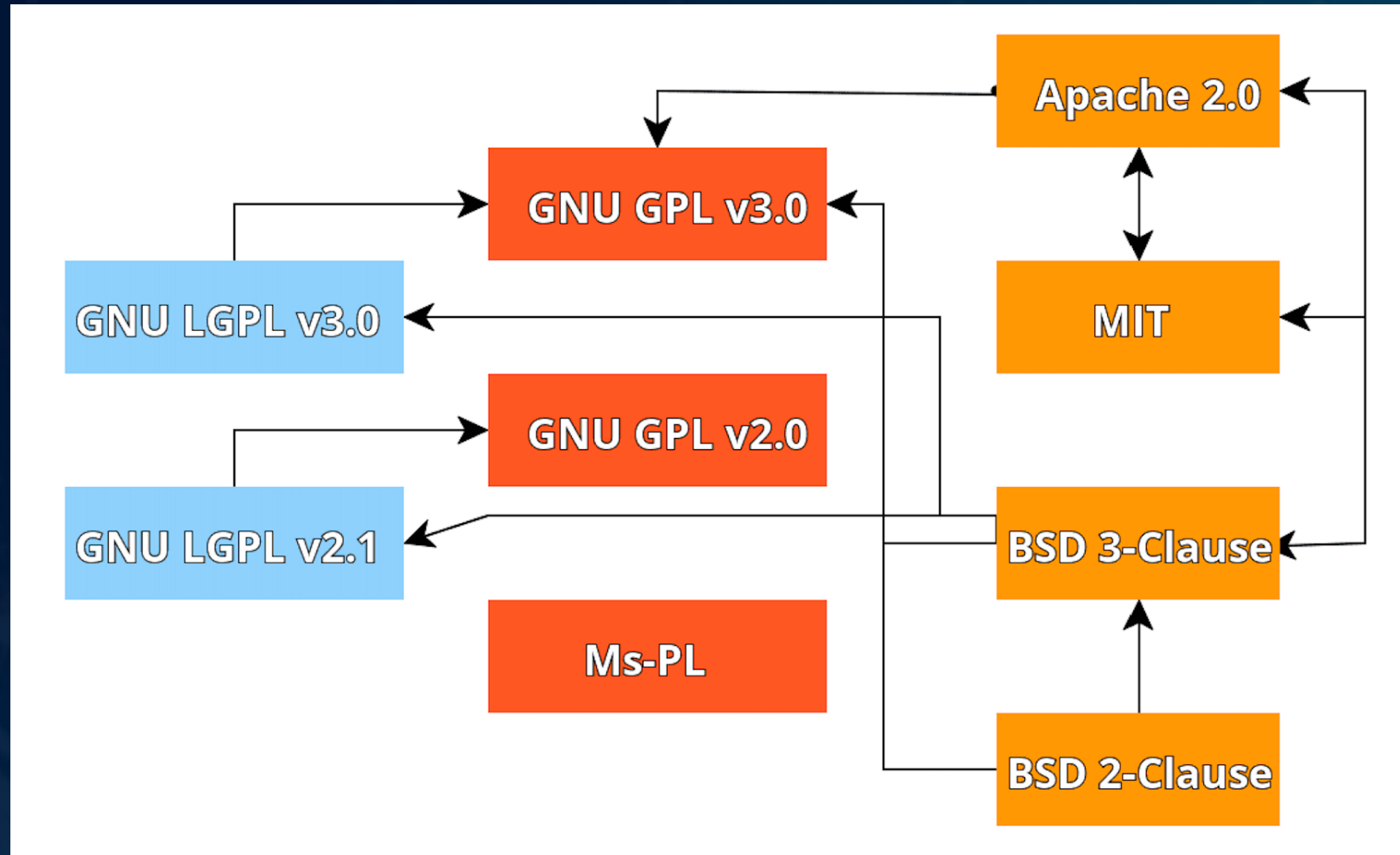
If the project is published without a license, the project cannot be used.

By default, the software is protected by exclusive copyright, and without a license, its usage is illegal, even if the project is published. The license grants permission to use, to copy, to distribute, or to modify the software without risk of infringement if the terms are met.

Compatibility of licenses

Black Duck Audit Services found that 53% of audited codebases in 2021 contained open-source code with conflicting licenses. 20% had open-source projects without licenses or custom licenses. In general, 97% of commercial code contains various parts and open-source projects. Most licenses protect and insure authors from possible lawsuits or damages that may be caused during the use of open-source components and projects in commercial products.

Compatibility of licenses



Add multiple licenses to a GitHub project

For multi-licensing in GitHub, you must name your license file with the keyword ***License*** or ***COPYING***; for example, ***License.BSD***, ***License_MIT***, and so on. Add related license text inside this file and place the license file or files in the root directory of your project.

An excellent example of how to organize multiple licenses can be found at [RocksDB](#).

Add multiple licenses to a GitHub project

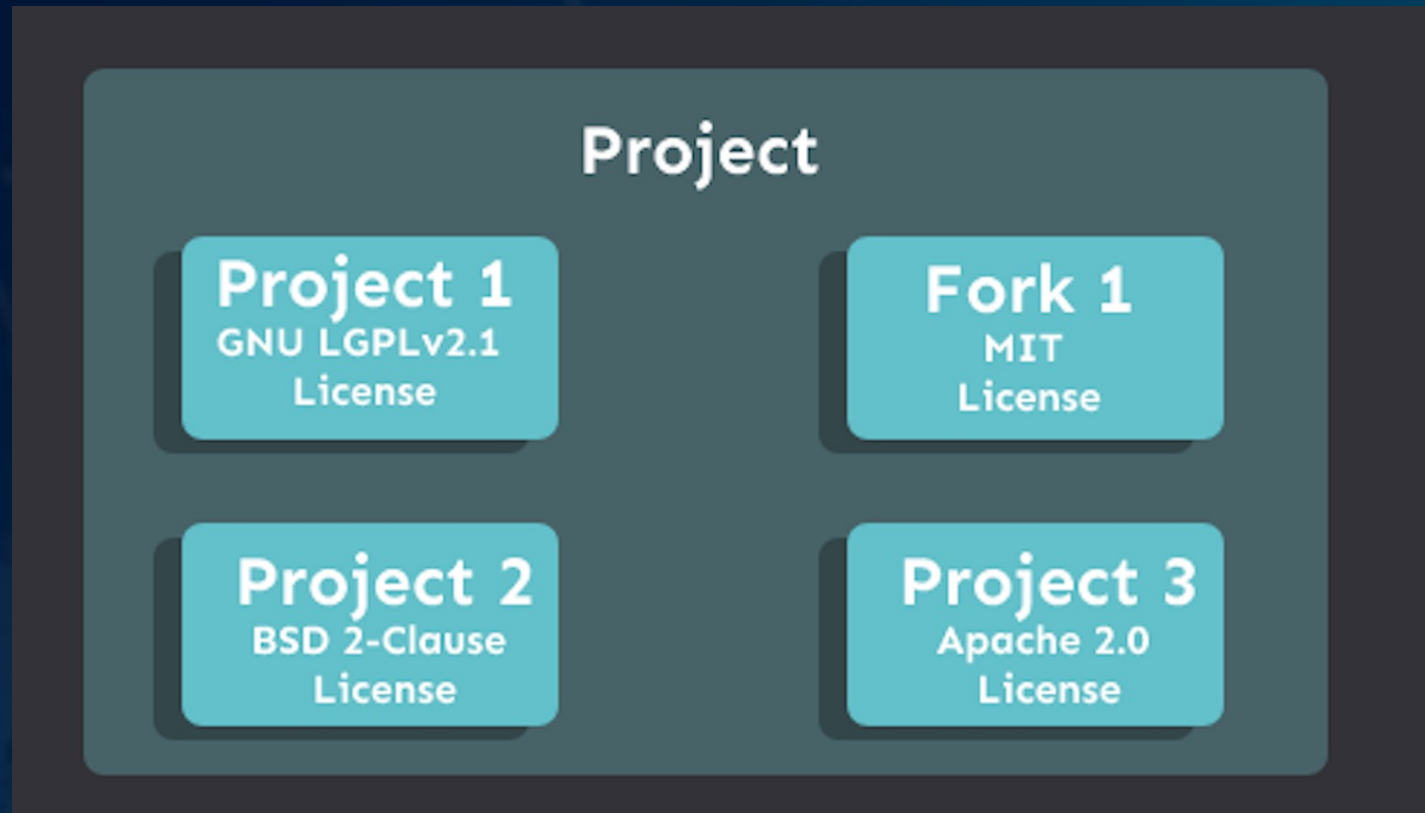
The screenshot shows the GitHub repository page for `facebook/rocksdb`. A modal window titled "Licenses found" is open, displaying the following information:

- GPL-2.0**
COPYING
- Apache-2.0**
LICENSE.Apache
- Unknown**
LICENSE.leveldb

The background shows the repository's file tree, including folders like `.circleci`, `.github/workflows`, `buckifier`, `build_tools`, `cache`, `cmake`, `coverage`, and `db`. The right sidebar contains the "About" section, which includes a description: "A library that provides an embeddable, persistent key-value store for fast storage." and a link to `rocksdb.org`. It also lists tags like `database` and `storage-engine`, and shows statistics such as 24.4k stars and 1k watching.

Multi-licensed project with forks

The project includes a fork or part of another project with different licenses



Multi-licensed project with forks

When your open source project contains forks of other projects or uses project code with different licenses and copyrights, create a separate directory where you place the licenses of the projects that are used in your project. Refer to the following examples:

Kubernetes -

<https://github.com/kubernetes/kubernetes/tree/master/LICENSES>

Elasticsearch client -

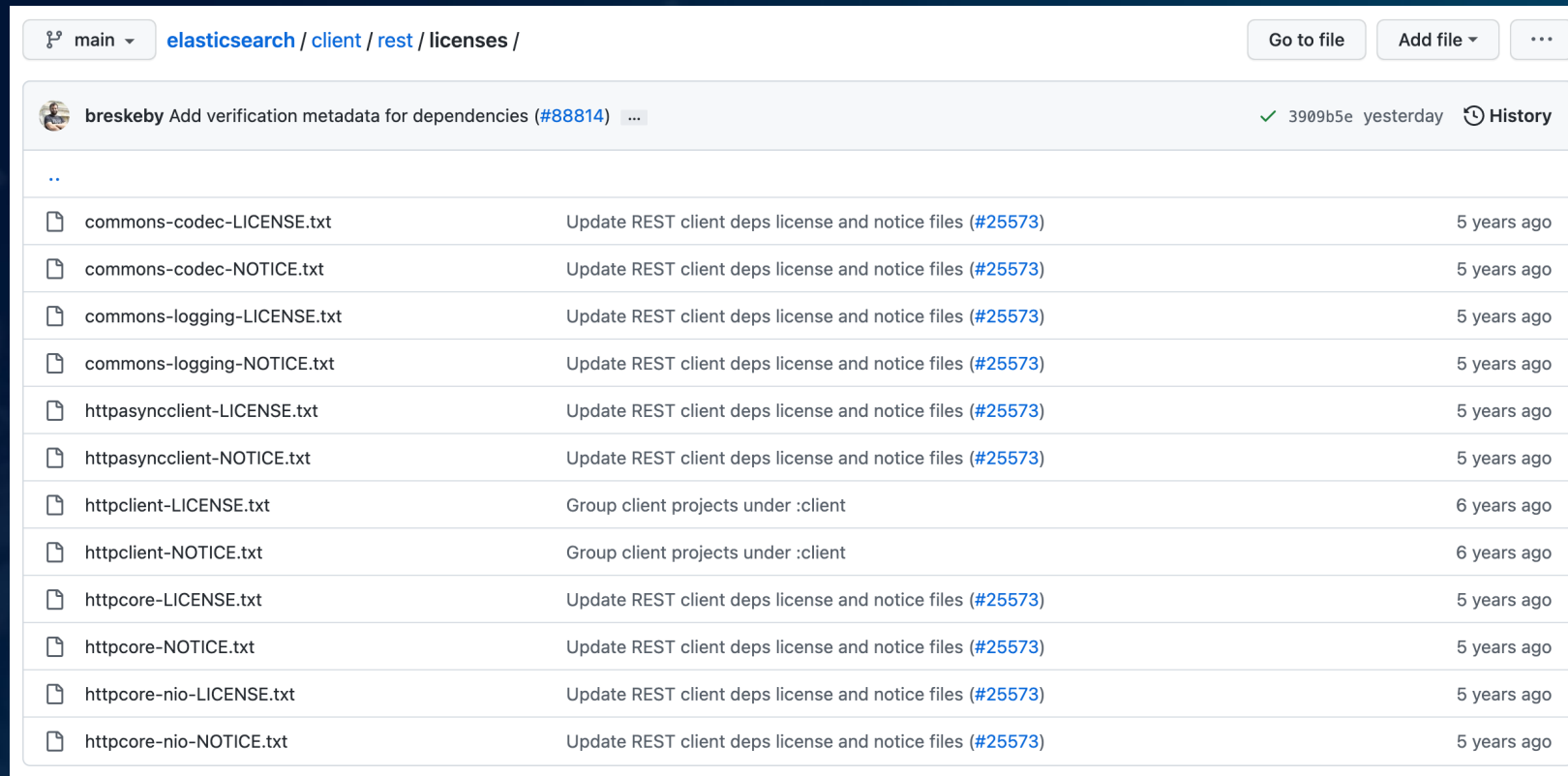
<https://github.com/elastic/elasticsearch/tree/main/client/rest/licenses>

CockroachDB -

<https://github.com/cockroachdb/cockroach/blob/master/LICENSE>

Multi-licensed project with forks

The following diagram shows an example of organizing information about licenses that are used in different parts of Elasticsearch:



File Name	Commit Message	Commit Hash	Time Ago
..			
commons-codec-LICENSE.txt	Update REST client deps license and notice files (#25573)	3909b5e	5 years ago
commons-codec-NOTICE.txt	Update REST client deps license and notice files (#25573)	3909b5e	5 years ago
commons-logging-LICENSE.txt	Update REST client deps license and notice files (#25573)	3909b5e	5 years ago
commons-logging-NOTICE.txt	Update REST client deps license and notice files (#25573)	3909b5e	5 years ago
httpasyncclient-LICENSE.txt	Update REST client deps license and notice files (#25573)	3909b5e	5 years ago
httpasyncclient-NOTICE.txt	Update REST client deps license and notice files (#25573)	3909b5e	5 years ago
httpclient-LICENSE.txt	Group client projects under :client		6 years ago
httpclient-NOTICE.txt	Group client projects under :client		6 years ago
httpcore-LICENSE.txt	Update REST client deps license and notice files (#25573)	3909b5e	5 years ago
httpcore-NOTICE.txt	Update REST client deps license and notice files (#25573)	3909b5e	5 years ago
httpcore-nio-LICENSE.txt	Update REST client deps license and notice files (#25573)	3909b5e	5 years ago
httpcore-nio-NOTICE.txt	Update REST client deps license and notice files (#25573)	3909b5e	5 years ago

License and copyright information

```
Executable File | 10 lines (7 sloc) | 154 Bytes  
  
1  #  
2  # Copyright (c) 2019 Cisco Systems  
3  # Licensed under the MIT License  
4  #  
5  
6  from django.apps import AppConfig  
7  
8  
9  class AppConfig(AppConfig):  
10     name = 'app'
```

About changing the license

Can a project be relicensed under a different license?

Yes, but the license change must be agreed upon by all project contributors, or if you are the sole author of a project and have accepted no contributions from third parties, you are free to relicense your project whenever or however you wish. This can even include changes solely to the README file. You can the most easily make the changes at the beginning of the project, when you are the only sole contributor. You can even change the license to a proprietary license, but such a change is not retroactive. Accordingly, all previous versions and releases can be used with the licenses in place at that time.

About changing the license

Facebook was using a BSD license plus their custom Additional Grant of Patent Rights. License was changed to MIT on September 26, 2017, and the Patent grant was deleted.

About changing the license

The screenshot shows a GitHub commit page for the file LICENSE. The commit was made by 'sophiebits' on Sep 26, 2017. The commit message is 'Showing 13 changed files with 27 additions and 78 deletions.' The file 'LICENSE' is highlighted in the left sidebar. The main content shows a diff view of the LICENSE file. The diff indicates that the license was changed from BSD to MIT. The new MIT license text is shown in green, and the old BSD license text is shown in red. The diff shows that the BSD license was removed and the MIT license was added. The MIT license text is as follows:

```
... .. @@ -1,31 +1,21 @@
1 - BSD License
2 -
3 - For React software
4 2
5 3 Copyright (c) 2013-present, Facebook, Inc.
6 - All rights reserved.
7 -
8 - Redistribution and use in source and binary forms, with or without modification,
9 - are permitted provided that the following conditions are met:
10 -
11 - * Redistributions of source code must retain the above copyright notice, this
12 - list of conditions and the following disclaimer.
13 4
14 - * Redistributions in binary form must reproduce the above copyright notice,
15 - this list of conditions and the following disclaimer in the documentation
16 - and/or other materials provided with the distribution.
17 11
18 - * Neither the name Facebook nor the names of its contributors may be used to
19 - endorse or promote products derived from this software without specific
20 - prior written permission.
```

Open Source Policies in Commercial Companies

Some companies create their licensing policies. The policies describe procedures and requirements for publishing projects. In addition, there are also requirements for project licenses that can be used in the company. There may also be lists of valid and invalid licenses (for example, block, allow list).

Open Source Policies in Commercial Companies

I give an example of a list of licenses with a level of risk relative to use in proprietary software. The greater the risk, the greater the problem of using adequately licensed components in your proprietary (commercial) software.

Risk	License	
High	Microsoft Reciprocal License (MS-RL)	●
	GNU Lesser General Public License (LGPL) 2.1, 3.0	●
	GNU General Public License (GPL) 2.0, 3.0	●
Low	MIT License	●
	Apache License 2.0	●
	2-Clause BSD License, 3-Clause BSD License	●
Medium	Microsoft Public License (MS-PL)	●
	Eclipse Public License (EPL)	●
	Artistic License (Perl)	●

Open Source Policies in Commercial Companies

For StackOverflow users, it will be interesting to know that according to the Terms of Service, all content created on the platform (including questions and answers) is licensed under Attribution-ShareAlike 4.0 International (CC BY-SA 4.0,). Using StackOverflow snippets can be a problem for your company's legal department.



Tools for managing open-source license

The screenshot shows a web interface for managing dependencies. At the top, it displays '18 Dependencies' and includes filters for license and source, a 'Flagged' checkbox, and buttons for 'Add Dependency' and 'Export'. A search bar is also present. Below the header, a list of dependencies is shown under the heading 'DIRECT DEPENDENCIES (18)'. Each entry includes a green checkmark, the package name, version, and a 'Pip' icon. The dependencies listed are: aiohttp (3.6.2), async-timeout (3.0.1), attrs (20.2.0), certifi (2020.6.20), chardet (3.0.4), and click (7.1.2). The certifi and chardet entries are highlighted in red and marked with 'policy flag' icons. The interface also shows license information for each package, such as Apache-2.0, MIT, MPL-2.0, and BSD-3-Clause, ISC.

<https://fossa.com/>

<https://www.mend.io/open-source-license-compliance/>

<https://snyk.io/product/open-source-security-management/license-compliance/>

Thanks



https://twitter.com/alex_dev_k
<https://github.com/oborys>