Advanced setup of the CodeQL CLI

In this article

You can modify your CodeQL CLI setup to use a local checkout of the CodeQL repository for analysis, set up multiple versions of the CodeQL CLI, and analyze databases you have downloaded from GitHub.com.

GitHub CodeQL is licensed on a per-user basis upon installation. You can use CodeQL only for certain tasks under the license restrictions. For more information, see "About the CodeQL CLI." If you have a GitHub Advanced Security license, you can use CodeQL for automated analysis, continuous integration, and continuous delivery. For more information, see "About GitHub Advanced Security."

About advanced setup of the CodeQL CLI

If you plan to use CodeQL for more than just code scanning, you may prefer an advanced setup of the CodeQL CLI.

- If you want to contribute to open source shared CodeQL queries, you may prefer working with the CodeQL source code directly.
- If you want to use the latest CodeQL features to generate code scanning alerts for a codebase, but also want to analyze another codebase that is only compatible with a specific version of the CodeQL CLI, you may want to install multiple versions of the CodeQL CLI.
- If you are researching or developing queries, you may want to download interesting or unique databases from GitHub.com.

For information on the most simple setup of the CodeQL CLI, see "Setting up the CodeQL CLI."

Checking out the CodeQL source code directly

Some users prefer working with CodeQL query sources directly in order to work on or contribute to the Open Source shared queries. In order to do this, the following steps are recommended.

1. Download the CodeQL CLI zip

The CodeQL CLI download package is a zip archive containing tools, scripts, and various CodeQL-specific files. If you don’t have a GitHub Enterprise license then, by downloading this archive, you are agreeing to the GitHub CodeQL Terms and Conditions.

You should download the CodeQL bundle from https://github.com/github/codeql-action/releases. The bundle contains:

- CodeQL CLI product
- A compatible version of the queries and libraries from https://github.com/github/codeql
- Precompiled versions of all the queries included in the bundle

Download information for macOS "Catalina" (or newer) users

From macOS version 10.15 ("Catalina") onwards you need to ensure that your web browser does not automatically extract zip files. If you use Safari, complete the following steps before downloading the CodeQL CLI zip archive:

1. Open Safari.
2. From the Safari menu, select **Preferences...** or **Settings...** (version 13 "Ventura" onwards).
3. Click the **General** Tab.
4. Ensure the check-box labeled **Open "safe" files after downloading** is unchecked.

2. Create a new CodeQL directory

Create a new directory where you can place the CLI and any queries and libraries you want to use. For example, `$HOME/codeql-home`.

The CLI's built-in search operations automatically look in all of its sibling directories for the files used in database creation and analysis. Keeping these components in their own directory prevents the CLI searching unrelated sibling directories while ensuring all files are available without specifying any further options on the command line.

3. Obtain a local copy of the CodeQL queries

The CodeQL repository contains the queries and libraries required for CodeQL analysis of all supported languages. Clone a copy of this repository into `codeql-home`.

By default, the root of the cloned repository will be called `codeql`. Rename this folder `codeql-repo` to avoid conflicting with the CodeQL CLI that you will extract in step 1. If you use git on the command line, you can clone and rename the repository in a single step by running `git clone git@github.com:github/codeql.git codeql-repo` in the `codeql-home` folder.

Within this repository, the queries and libraries are organized into CodeQL packs. Along with the queries themselves, CodeQL packs contain important metadata that tells the CodeQL CLI how to process the query files. For more information, see "Creating and working with CodeQL packs."

Note: There are different versions of the CodeQL queries available for different users. Check out the correct version for your use case:

- For the queries that are intended to be used with the latest CodeQL CLI release, check out the branch tagged `codeql-cli/latest`. You should use this branch for databases you've built using the CodeQL CLI or recently downloaded from GitHub.com.
- For the most up to date CodeQL queries, check out the `main` branch. This branch represents the very latest version of CodeQL's analysis.

4. Extract the zip archive

For Linux, Windows, and macOS users (version 10.14 "Mojave", and earlier) simply extract the zip archive into the directory you created in step 2.

For example, if the path to your copy of the CodeQL repository is `$HOME/codeql-home/codeql-repo`, then extract the CLI into `$HOME/codeql-home/`.

Extraction information for macOS "Catalina" (or newer) users

macOS "Catalina", "Big Sur", "Monterey", or "Ventura" users should run the following commands in the Terminal, where `${extraction-root}` is the path to the directory where you will extract the CodeQL CLI zip archive:

1. `mv ~/Downloads/codeql\*.zip ${extraction-root}`
2. `cd ${extraction-root}`
3. `/usr/bin/xattr -c codeql\*.zip`
4. `unzip codeql\*.zip`

5. Launch `codeql`

Once extracted, you can run CodeQL processes by running the `codeql` executable in a couple of ways:

- By executing `<extraction-root>/codeql/codeql`, where `<extraction-root>` is the folder where you extracted the CodeQL CLI package.
- By adding `<extraction-root>/codeql` to your `PATH`, so that you can run the executable as just `codeql`.

At this point, you can execute CodeQL commands. For a full list of the CodeQL CLI commands, see "CodeQL CLI commands manual."

6. Verify your CodeQL CLI setup

CodeQL CLI has subcommands you can execute to verify that you are correctly set up to create and analyze databases:

- Run `codeql resolve languages` to show which languages are available for database creation. This will list the languages supported by default in your CodeQL CLI package.
- Run `codeql resolve qlpacks` to show which CodeQL packs the CLI can find. This will display the names of all the CodeQL packs directly available to the CodeQL CLI. This should include:
- Query packs for each supported language, for example, `codeql/{language}-queries`. These packs contain the standard queries that will be run for each analysis.
- Library packs for each supported language, for example, `codeql/{language}-all`. These packs contain query libraries, such as control flow and data flow libraries, that may be useful to query writers.
- Example packs for each supported language, for example, `codeql/{language}-examples`. These packs contain useful snippets of CodeQL that query writers may find useful.
- Legacy packs that ensure custom queries and libraries created using older products are compatible with your version of CodeQL.

Using two versions of the CodeQL CLI

If you want to use the latest CodeQL features to execute queries or CodeQL tests, but also want to prepare databases that are compatible with a specific version of CodeQL code scanning on GitHub Enterprise Server, you may need to install two versions of the CLI. You can download the versions of the CodeQL CLI that you want, and unpack both CLI archives in the same parent directory.

Downloading databases from GitHub.com

GitHub stores CodeQL databases for over 200,000 repos on GitHub.com, which you can download using the REST API. The list of repos is constantly growing and evolving to make sure that it includes the most interesting codebases for security research.

You can also analyze databases from GitHub.com using the CodeQL for VS Code extension. For more information, see "Analyzing your projects."

You can check if a repository has any CodeQL databases available for download using the `/repos/<owner>/<repo>/code-scanning/codeql/databases` endpoint. For example, to check for CodeQL databases using the GitHub CLI you would run:

```
gh api /repos/<owner>/<repo>/code-scanning/codeql/databases
```

This command returns information about any CodeQL databases that are available for a repository, including the language the database represents, and when the database was last updated. If no CodeQL databases are available, the response is empty.

When you have confirmed that a CodeQL database exists for the language you are interested in, you can download it using the following command:

```
gh api /repos/<owner>/<repo>/code-scanning/codeql/databases/<language> -H
'Accept: application/zip' > path/to/local/database.zip
```

For more information, see the documentation for the Get CodeQL database endpoint.

Before running an analysis with the CodeQL CLI, you must unzip the databases.