

# The `build2` Repository Interface

Copyright © 2014-2025 the build2 authors.

Permission is granted to copy, distribute and/or modify this document under the terms of the MIT License.

Revision 0.18, May 2025

This revision of the document describes the `build2` repository interface 0.18.x series.



# Table of Contents

Preface . . . . .	1
1 Package Submission . . . . .	1
1.1 Submission Request Manifest . . . . .	3
1.2 Submission Result Manifest . . . . .	3
2 Package CI . . . . .	4
2.1 CI Request Manifest . . . . .	6
2.2 CI Overrides Manifest . . . . .	7
2.3 CI Result Manifest . . . . .	7
3 Build Artifacts Upload . . . . .	8
3.1 Upload Request Manifest . . . . .	10
3.2 Upload Result Manifest . . . . .	11
4 Package Review Submission . . . . .	11
4.1 Package Review Manifest . . . . .	11
5 GitHub CI Integration . . . . .	12
5.1 GitHub CI Background . . . . .	12
5.2 Enabling CI Integration on GitHub Repository . . . . .	15
5.2.1 Adding classic branch protection rule . . . . .	16
5.2.2 Adding branch ruleset . . . . .	16



# Preface

This document describes `brep`, the `build2` package repository web interface. For the command line interface of `brep` utilities refer to the **`brep-load(1)`**, **`brep-clean(1)`**, **`brep-migrate(1)`**, and **`brep-monitor(1)`** man pages.

## 1 Package Submission

The package submission functionality allows uploading of package archives as well as additional, repository-specific information via the HTTP POST method using the `multipart/form-data` content type. The implementation in `brep` only handles uploading as well as basic verification (checksum, duplicates) expecting the rest of the submission and publishing logic to be handled by a separate entity according to the repository policy. Such an entity can be notified by `brep` about a new submission as an invocation of the *handler program* (as part of the HTTP request) and/or via email. It could also be a separate process that monitors the upload data directory.

The submission request without any parameters is treated as the submission form request. If `submit-form` is configured, then such a form is generated and returned. Otherwise, such a request is treated as an invalid submission (missing parameters).

For each submission request `brep` performs the following steps.

1. Verify submission size limit.

The submission form-data payload size must not exceed `submit-max-size`.

2. Verify the required `archive` and `sha256sum` parameters are present.

The `archive` parameter must be the package archive upload while `sha256sum` must be its 64 characters SHA256 checksum calculated in the binary mode.

3. Verify other parameters are valid manifest name/value pairs.

The value can only contain UTF-8 encoded Unicode graphic characters as well as tab (`\t`), carriage return (`\r`), and line feed (`\n`).

4. Check for a duplicate submission.

Each submission is saved as a subdirectory in the `submit-data` directory with a 12-character abbreviated checksum as its name.

5. Save the package archive into a temporary directory and verify its checksum.

A temporary subdirectory is created in the `submit-temp` directory, the package archive is saved into it using the submitted name, and its checksum is calculated and compared to the submitted checksum.

## 6. Save the submission request manifest into the temporary directory.

The submission request manifest is saved as `request.manifest` into the temporary subdirectory next to the archive.

## 7. Make the temporary submission directory permanent.

Move/rename the temporary submission subdirectory to `submit-data` as an atomic operation using the 12-character abbreviated checksum as its new name. If such a directory already exist, then this is a duplicate submission.

## 8. Invoke the submission handler program.

If `submit-handler` is configured, invoke the handler program passing to it additional arguments specified with `submit-handler-argument` (if any) followed by the absolute path to the submission directory.

The handler program is expected to write the submission result manifest to `stdout` and terminate with the zero exit status. A non-zero exit status is treated as an internal error. The handler program's `stderr` is logged.

Note that the handler program should report temporary server errors (service overload, network connectivity loss, etc.) via the submission result manifest status values in the [500-599] range (HTTP server error) rather than via a non-zero exit status.

The handler program assumes ownership of the submission directory and can move/remove it. If after the handler program terminates the submission directory still exists, then it is handled by `brep` depending on the handler process exit status and the submission result manifest status value. If the process has terminated abnormally or with a non-zero exit status or the result manifest status is in the [500-599] range (HTTP server error), then the directory is saved for troubleshooting by appending the `.fail` extension followed by a numeric extension to its name (for example, `ff5a1a53d318.fail.1`). Otherwise, if the status is in the [400-499] range (HTTP client error), then the directory is removed. If the directory is left in place by the handler or is saved for troubleshooting, then the submission result manifest is saved as `result.manifest` into this directory, next to the request manifest and archive.

If `submit-handler-timeout` is configured and the handler program does not exit in the allotted time, then it is killed and its termination is treated as abnormal.

If the handler program is not specified, then the following submission result manifest is implied:

```
status: 200
message: package submission is queued
reference: <abbrev-checksum>
```

## 9. Send the submission email.

If `submit-email` is configured, send an email to this address containing the submission request manifest and the submission result manifest.

## 10. Respond to the client.

Respond to the client with the submission result manifest and its `status` value as the HTTP status code.

Check violations (max size, duplicate submissions, etc) that are explicitly mentioned above are always reported with the submission result manifest. Other errors (for example, internal server errors) might be reported with unformatted text, including HTML.

If the submission request contains the `simulate` parameter, then the submission service simulates the specified outcome of the submission process without actually performing any externally visible actions (e.g., publishing the package, notifying the submitter, etc). Note that the package submission email (`submit-email`) is not sent for simulated submissions.

Pre-defined simulation outcome values are `internal-error-text`, `internal-error-html`, `duplicate-archive`, and `success`. The simulation outcome is included into the submission request manifest and the handler program must at least handle `success` but may recognize additional outcomes.

## 1.1 Submission Request Manifest

The submission request manifest starts with the below values and in that order optionally followed by additional values in the unspecified order corresponding to the custom request parameters.

```
archive: <name>
sha256sum: <sum>
timestamp: <date-time>
[simulate]: <outcome>
[client-ip]: <string>
[user-agent]: <string>
```

The `timestamp` value is in the ISO-8601 `<YYYY>-<MM>-<DD>T<hh>:<mm>:<ss>Z` form (always UTC). Note also that `client-ip` can be IPv4 or IPv6.

## 1.2 Submission Result Manifest

The submission result manifest starts with the below values and in that order optionally followed by additional values if returned by the handler program. If the submission is successful, then the `reference` value must be present and contain a string that can be used to identify this submission (for example, the abbreviated checksum).

```
status: <http-code>
message: <string>
[reference]: <string>
```

## 2 Package CI

The CI functionality allows submission of package CI requests as well as additional, repository-specific information via the HTTP GET and POST methods using the `application/x-www-form-urlencoded` or `multipart/form-data` parameters encoding. The implementation in `brep` only handles reception as well as basic parameter verification expecting the rest of the CI logic to be handled by a separate entity according to the repository policy. Such an entity can be notified by `brep` about a new CI request as an invocation of the *handler program* (as part of the HTTP request) and/or via email. It could also be a separate process that monitors the CI data directory.

The CI request without any parameters is treated as the CI form request. If `ci-form` is configured, then such a form is generated and returned. Otherwise, such a request is treated as an invalid CI request (missing parameters).

For each CI request `brep` performs the following steps.

1. Verify the required `repository` and optional package parameters.

The `repository` parameter is the remote `bpkg` repository location that contains the packages to be tested. If one or more package parameters are present, then only the specified packages are tested. If no package parameters are specified, then all the packages present in the repository (but excluding complement repositories) are tested.

Each package parameter can specify either just the package name, in which case all the versions of this package present in the repository will be tested, or both the name and version in the `<name>/<version>` form (for example, `libhello/1.2.3`).

2. Verify the optional `overrides` parameter.

The `overrides` parameter, if specified, must be the CI overrides manifest upload.

3. Verify other parameters are valid manifest name/value pairs.

The value can only contain UTF-8 encoded Unicode graphic characters as well as tab (`\t`), carriage return (`\r`), and line feed (`\n`).

4. Generate CI request id and create request directory.

For each CI request a unique id (UUID) is generated and a request subdirectory is created in the `ci-data` directory with this id as its name.

5. Save the CI request manifest into the request directory.

The CI request manifest is saved as `request.manifest` into the request subdirectory created on the previous step.



## 6. Save the CI overrides manifest into the request directory.

If the CI overrides manifest is uploaded, then it is saved as `overrides.manifest` into the request subdirectory.

## 7. Invoke the CI handler program.

If `ci-handler` is configured, invoke the handler program passing to it additional arguments specified with `ci-handler-argument` (if any) followed by the absolute path to the CI request directory.

The handler program is expected to write the CI result manifest to `stdout` and terminate with the zero exit status. A non-zero exit status is treated as an internal error. The handler program's `stderr` is logged.

Note that the handler program should report temporary server errors (service overload, network connectivity loss, etc.) via the CI result manifest status values in the [500-599] range (HTTP server error) rather than via a non-zero exit status.

The handler program assumes ownership of the CI request directory and can move/remove it. If after the handler program terminates the request directory still exists, then it is handled by `brep` depending on the handler process exit status and the CI result manifest status value. If the process has terminated abnormally or with a non-zero exit status or the result manifest status is in the [500-599] range (HTTP server error), then the directory is saved for troubleshooting by appending the `.fail` extension to its name. Otherwise, if the status is in the [400-499] range (HTTP client error), then the directory is removed. If the directory is left in place by the handler or is saved for troubleshooting, then the CI result manifest is saved as `result.manifest` into this directory, next to the request manifest.

If `ci-handler-timeout` is configured and the handler program does not exit in the allotted time, then it is killed and its termination is treated as abnormal.

If the handler program is not specified, then the following CI result manifest is implied:

```
status: 200
message: CI request is queued
reference: <request-id>
```

## 8. Send the CI request email.

If `ci-email` is configured, send an email to this address containing the CI request manifest, the potentially empty CI overrides manifest, and the CI result manifest.

## 9. Respond to the client.

Respond to the client with the CI result manifest and its `status` value as the HTTP status code.

Check violations that are explicitly mentioned above are always reported with the CI result manifest. Other errors (for example, internal server errors) might be reported with unformatted text, including HTML.

If the CI request contains the `interactive` parameter, then the CI service provides the execution environment login information for each test and stops them at the specified breakpoint.

Pre-defined breakpoint ids are `error` and `warning`. The breakpoint id is included into the CI request manifest and the CI service must at least handle `error` but may recognize additional ids (build phase/command identifiers, etc).

If the CI request contains the `simulate` parameter, then the CI service simulates the specified outcome of the CI process without actually performing any externally visible actions (e.g., testing the package, publishing the result, etc). Note that the CI request email (`ci-email`) is not sent for simulated requests.

Pre-defined simulation outcome values are `internal-error-text`, `internal-error-html`, and `success`. The simulation outcome is included into the CI request manifest and the handler program must at least handle `success` but may recognize additional outcomes.

## 2.1 CI Request Manifest

The CI request manifest starts with the below values and in that order optionally followed by additional values in the unspecified order corresponding to the custom request parameters.

```
id: <request-id>
repository: <url>
[package]: <name>[/<version>]
[interactive]: <breakpoint>
[simulate]: <outcome>
timestamp: <date-time>
[client-ip]: <string>
[user-agent]: <string>
[service-id]: <string>
[service-type]: <string>
[service-data]: <string>
[service-action]: <action>
```

The `package` value can be repeated multiple times. The `timestamp` value is in the ISO-8601 `<YYYY>-<MM>-<DD>T<hh>:<mm>:<ss>Z` form (always UTC). Note also that `client-ip` can be IPv4 or IPv6.

Note that some CI service implementations may serve as backends for third-party services. The latter may initiate CI tasks, providing all the required information via some custom protocol, and expect the CI service to notify it about the progress. In this case the third-party service type as well as optionally the third-party id and custom state data can be communicated to the underlying CI handler program via the respective `service-*` manifest values. Also note that normally a third-party service has all the required information (repository URL,

etc) available at the time of the CI task initiation, in which case the `start` value is specified for the `service-action` manifest value. If that's not the case, the CI task is only created at the time of the initiation without calling the CI handler program. In this case the CI handler is called later, when all the required information is asynchronously gathered by the service. In this case the `load` value is specified for the `service-action` manifest value.

## 2.2 CI Overrides Manifest

The CI overrides manifest is a package manifest fragment that should be applied to all the packages being tested. The contained values override the whole value groups they belong to, resetting all the group values prior to being applied. Currently, only the following value groups can be overridden:

```
build-email build-{warning,error}-email
builds build-{include,exclude}
*-builds *-build-{include,exclude}
*-build-config
```

For the package configuration-specific build constraint overrides the corresponding configuration must exist in the package manifest. In contrast, the package configuration override (**\*-build-config**) adds a new configuration if it doesn't exist and updates the arguments of the existing configuration otherwise. In the former case, all the potential build constraint overrides for such a newly added configuration must follow the corresponding **\*-build-config** override.

Note that the build constraints group values (both common and build package configuration-specific) are overridden hierarchically so that the **[\*-]build-{include,exclude}** overrides don't affect the respective **[\*-]builds** values.

Note also that the common and build package configuration-specific build constraints group value overrides are mutually exclusive. If the common build constraints are overridden, then all the configuration-specific constraints are removed. Otherwise, if any configuration-specific constraints are overridden, then for the remaining configurations the build constraints are reset to **builds: none**.

See Package Manifest for details on these values.

## 2.3 CI Result Manifest

The CI result manifest starts with the below values and in that order optionally followed by additional values if returned by the handler program. If the CI request is successful, then the `reference` value must be present and contain a string that can be used to identify this request (for example, the CI request id).

```
status: <http-code>
message: <string>
[reference]: <string>
```

## 3 Build Artifacts Upload

The build artifacts upload functionality allows uploading archives of files generated as a byproduct of the package builds. Such archives as well as additional, repository-specific information can optionally be uploaded by the automated build bots via the HTTP POST method using the `multipart/form-data` content type (see the `bbot` documentation for details). The implementation in `brep` only handles uploading as well as basic actions and verification (build session resolution, agent authentication, checksum verification) expecting the rest of the upload logic to be handled by a separate entity according to the repository policy. Such an entity can be notified by `brep` about a new upload as an invocation of the *handler program* (as part of the HTTP request) and/or via email. It could also be a separate process that monitors the upload data directory.

For each upload request `brep` performs the following steps.

1. Determine upload type.

The upload type must be passed via the `upload` parameter in the query component of the request URL.

2. Verify upload size limit.

The upload form-data payload size must not exceed `upload-max-size` specific for this upload type.

3. Verify the required `session`, `instance`, `archive`, and `sha256sum` parameters are present. If `brep` is configured to perform agent authentication, then verify that the `challenge` parameter is also present. See the Result Request Manifest for semantics of the `session` and `challenge` parameters.

The `archive` parameter must be the build artifacts archive upload while `sha256sum` must be its 64 characters SHA256 checksum calculated in the binary mode.

4. Verify other parameters are valid manifest name/value pairs.

The value can only contain UTF-8 encoded Unicode graphic characters as well as tab (`\t`), carriage return (`\r`), and line feed (`\n`).

5. Resolve the session.

Resolve the `session` parameter value to the actual package build information.

6. Authenticate the build bot agent.

Use the `challenge` parameter value and the resolved package build information to authenticate the agent, if configured to do so.

7. Generate upload request id and create request directory.

For each upload request a unique id (UUID) is generated and a request subdirectory is created in the `upload-data` directory with this id as its name.

8. Save the upload archive into the request directory and verify its checksum.

The archive is saved using the submitted name, and its checksum is calculated and compared to the submitted checksum.

9. Save the upload request manifest into the request directory.

The upload request manifest is saved as `request.manifest` into the request subdirectory next to the archive.

10. Invoke the upload handler program.

If `upload-handler` is configured, invoke the handler program passing to it additional arguments specified with `upload-handler-argument` (if any) followed by the absolute path to the upload request directory.

The handler program is expected to write the upload result manifest to `stdout` and terminate with the zero exit status. A non-zero exit status is treated as an internal error. The handler program's `stderr` is logged.

Note that the handler program should report temporary server errors (service overload, network connectivity loss, etc.) via the upload result manifest status values in the [500-599] range (HTTP server error) rather than via a non-zero exit status.

The handler program assumes ownership of the upload request directory and can move/remove it. If after the handler program terminates the request directory still exists, then it is handled by `brep` depending on the handler process exit status and the upload result manifest status value. If the process has terminated abnormally or with a non-zero exit status or the result manifest status is in the [500-599] range (HTTP server error), then the directory is saved for troubleshooting by appending the `.fail` extension to its name. Otherwise, if the status is in the [400-499] range (HTTP client error), then the directory is removed. If the directory is left in place by the handler or is saved for troubleshooting, then the upload result manifest is saved as `result.manifest` into this directory, next to the request manifest.

If `upload-handler-timeout` is configured and the handler program does not exit in the allotted time, then it is killed and its termination is treated as abnormal.

If the handler program is not specified, then the following upload result manifest is implied:

```
status: 200
message: <upload-type> upload is queued
reference: <request-id>
```

#### 11. Send the upload email.

If `upload-email` is configured, send an email to this address containing the upload request manifest and the upload result manifest.

#### 12. Respond to the client.

Respond to the client with the upload result manifest and its `status` value as the HTTP status code.

Check violations (max size, etc) that are explicitly mentioned above are always reported with the upload result manifest. Other errors (for example, internal server errors) might be reported with unformatted text, including HTML.

## 3.1 Upload Request Manifest

The upload request manifest starts with the below values and in that order optionally followed by additional values in the unspecified order corresponding to the custom request parameters.

```
id: <request-id>
session: <session-id>
instance: <name>
archive: <name>
sha256sum: <sum>
timestamp: <date-time>

name: <name>
version: <version>
project: <name>
target-config: <name>
package-config: <name>
target: <target-triplet>
[tenant]: <tenant-id>
toolchain-name: <name>
toolchain-version: <standard-version>
repository-name: <canonical-name>
machine-name: <name>
machine-summary: <text>
```

The timestamp value is in the ISO-8601 `<YYYY>-<MM>-<DD>T<hh>:<mm>:<ss>Z` form (always UTC).

## 3.2 Upload Result Manifest

The upload result manifest starts with the below values and in that order optionally followed by additional values if returned by the handler program. If the upload request is successful, then the `reference` value must be present and contain a string that can be used to identify this request (for example, the upload request id).

```
status: <http-code>
message: <string>
[reference]: <string>
```

## 4 Package Review Submission

### 4.1 Package Review Manifest

The package review manifest files are per version/revision and are normally stored on the filesystem along with other package metadata (like ownership information). Under the metadata root directory, a review manifest file has the following path:

```
<project>/<package>/<version>/reviews.manifest
```

For example:

```
hello/libhello/1.2.3+2/reviews.manifest
```

Note that review manifests are normally not removed when the corresponding package archive is removed (for example, as a result of a replacement with a revision) because reviews for subsequent versions may refer to review results of previous versions (see below).

The package review file is a manifest list with each manifest containing the below values in an unspecified order:

```
reviewed-by: <string>
result-<name>: pass|fail|unchanged
[base-version]: <version>
[details-url]: <url>
```

For example:

```
reviewed-by: John Doe <john@example.org>
result-build: fail
details-url: https://github.com/build2-packaging/hello/issues/1
```

The `reviewed-by` value identifies the reviewer. For example, a deployment policy may require a real name and email address when submitting a review.

The `result-<name>` values specify the review results for various aspects of the package. At least one result value must be present and duplicates for the same aspect name are not allowed. For example, a deployment may define the following aspect names: `build` (build system), `code` (implementation source code), `test` (tests), `doc` (documentation).

The `result-<name>` value must be one of `pass` (the review passed), `fail` (the review failed), and `unchanged` (the aspect in question hasn't changed compared to the previous version, which is identified with the `base-version` value; see below).

The `base-version` value identifies the previous version on which this review is based. The idea here is that when reviewing a new revision, a patch version, or even a minor version, it is often easier to review the difference between the two versions than to review everything from scratch. In such cases, if some aspects haven't changed since the previous version, then their results can be specified as `unchanged`. The `base-version` value must be present if at least one `result-<name>` value is `unchanged`.

The `details-url` value specifies a URL that contains the details of the review (issues identified, etc). It can only be absent if none of the `result-<name>` values are `fail` (a failed review needs an explanation of why it failed).

## 5 GitHub CI Integration

This chapter describes the integration of the Package CI functionality with GitHub.

### 5.1 GitHub CI Background

The GitHub CI model has a number of limitations that are important to understand in order to use the provided integration correctly. To understand the limitations, however, we first need to understand how the integration works, at least at the high level.

GitHub supports integration of third-party CI services into the repository workflow by allowing such third-party services to register for events (called *web hooks* in the GitHub terminology).

This mechanism should not be confused with GitHub Actions, which is a GitHub built-in CI service. As far as we understand, it uses ad hoc integration rather than the same integration mechanism as available to third-party CI services.

While there are many repository workflow events, for CI the only relevant ones are:

1. *Branch push* (BP), which is triggered when a new commit is pushed to a branch in your repository.
2. *Pull request* (PR), which is triggered when a new pull request is created on your repository. It is also triggered when new commits are added to the existing PR.

Another relevant event is *Merge queue*. However, merge queues are not yet supported by this integration.

In response to these events the third-party CI service is expected to start a number of CI jobs (called *checks* in the GitHub terminology) and then report their progress and results back to GitHub to be shown to the user, and, in case of PRs, to prevent them from being merged in case the result is unsuccessful.



More precisely, this prevention applies more generally to any attempt to merge or push an unchecked commit to a protected branch. For example, if the default branch is protected and you attempt to push to it a commit that hasn't been successfully checked, this attempt will fail. See the next section on setting branch protection rule.

Let's examine in more detail what exactly happens in case of a branch push and a pull request.

The branch push (BP) case is pretty straightforward: when you push a new commit to a branch in your repository, this commit is CI'ed by the third-party service and the result is associated with this commit. If you push another commit, the process repeats and you get a new set of CI results associated with the new commit. The important point here is that the CI results for each commit are associated with that commit id (called *head sha* in the GitHub terminology).

The pull request (PR) case is more complicated: the aim of a PR is to merge one or more commits from one branch (called *head branch* in the GitHub terminology) to another branch (called *base branch* in the GitHub terminology). If the base branch can be fast-forwarded to the head commit of the head branch, then we can CI this head commit and the result will be representative of the merge. However, if base cannot be fast-forwarded, then a general merge of the two branches must be performed, with potential conflict resolution, etc. And in this case the CI result for the head commit may not necessarily represent the result of the merge.

To support the general case (when the base branch cannot be fast-forwarded) GitHub creates a tentative merge commit (called *test merge commit* in the GitHub terminology) and expects the CI service to test that commit rather than the head commit (this is what most of the major CI integrations do). See [The Many SHAs of a GitHub Pull Request](#) for additional details.

While the PR case is more complicated, so far everything makes sense. But that ends once we understand what GitHub associates the CI result with in case of a PR. Since the CI service is expected to test the merge commit, it would make sense to associate the result of this test with the merge commit. Instead, GitHub expects the CI service to report it as associated with the head commit!

This strange decision by GitHub, which we will refer to as "head sharing", has two serious consequences for trusting CI results when making decisions about merging PRs.

Firstly, if the branch push and/or several pull requests share the same head commit, then they will share the CI result, regardless of the state of the PRs' base branches. Or, to put it another way, in the GitHub model there is a single CI result per head commit that is shared by all the BPs and PRs with this head commit.

Secondly, if the base branch of a PR moves, the CI result associated with the PR does not get invalidated (because the PR head hasn't changed).

Let's consider two representative examples of each case that show how the GitHub behavior can lead us to making wrong decisions. But before we do that, a last bit of terminology: we will distinguish between *local PRs*, those with the head branch from the same repository, and *remote PRs*, those with the head branch belonging to another user/organization (called *forked*

*PR* in the GitHub terminology).

The first representative example is a feature branch: we develop a feature in a branch of our repository and once it is ready, we create a local PR to merge it to the `master/main` branch. We typically go through the PR instead of merging our branch directly in order to have the changes reviewed by someone else. In this scenario, the head commit of our feature branch and of the PR we created will be the same, which means our PR will share the CI result with the feature branch push, which is presumably successful. This can lead us to merging the PR based on this result even though the merge commit of the PR may not have the same contents as the head commit of the result. For example, we may have forgotten to rebase our feature branch on the base branch (`master/main` in our example) before creating the PR and the base branch has moved while we developed the feature. Or the review may have taken some time and the base branch likewise has moved in the meantime. In both these cases while the changes to the base branch may not render our head commit unmergeable (for example, due to conflicts), they may render our changes uncompileable or otherwise buggy once merged.

The second representative example is a single remote PR: someone creates a PR with a feature or bugfix from their fork of our repository. There is no corresponding branch push for this PR's head commit in our repository so it sounds like there is only one place (the PR) where the CI result, if associated with this head commit, will be reported in our repository and so the head sharing should not be an issue, right? While it's true that *spatial* sharing, that is between BP and/or several PRs, is not an issue in this case, *temporal* sharing still is. Specifically, if the base branch moves before we examine the PR, we again may end up merging it based on the CI results that are not representative of the merge commit.

Hopefully you see the underlying theme by now: the only way to ensure correctness in the GitHub CI model is to make sure the PR's head and merge commits are the same, which is only the case when the PR base branch can be fast-forwarded to head.

Thankfully, GitHub provides a branch protection rule that prevents merging of a PR with the head branch behind base (we will refer to it as the *head-behind-base* protection). Enabling of this protection rule is a prerequisite for this CI integration to work correctly.

Note, however, that even with the head-behind-base protection enabled, some of the GitHub behavior can be counter-intuitive.

For one, GitHub does not prevent the CI build from starting if this protection rule is violated. While this integration checks the result of this protection rule and does not start the build if the head is behind, the CI result may already be available (if this head is shared with a branch push and/or another PR), in which case GitHub will show it. So you may end up with a violated head-behind-base protection but with a successful CI result.

Another surprising consequence of the head sharing is the instantaneous availability of the CI result, which may look suspicious. For example, if you create a PR from a local feature branch, you may immediately see the successful CI result because it is the same as for the branch push to the feature branch.

Finally note that the GitHub CI model is quite wasteful of CI resources in general and the head sharing makes this problem even worse. Specifically, GitHub CI builds every commit indiscriminately, regardless of what was changed. So a minor tweak to `README.md` will trigger a full rebuild even though nothing that needs building has changed. The head sharing issue makes the situation worse because the CI integration cannot easily cancel an in-progress build when a new commit is added to a PR because the result could be shared with a branch push or another PR. Nevertheless, this integration will attempt to cancel a stale build of a remote PR provided it's not (currently) shared.

## 5.2 Enabling CI Integration on GitHub Repository

To enable the CI integration on a GitHub repository, the corresponding GitHub App must be first installed into the user or organization account to which this repository belongs. To do this go to GitHub Marketplace and search for "build2 CI". This should bring the list of available `build2` CI Apps to choose from. Click on the desired App and scroll to the bottom to install it.

Once this is done, go to the account settings and open the "Applications" tab. There you should see the App you just installed. Click on the "Configure" button next to it and in the "Repository Access" section list the repositories you wish to CI. Then click "Save".

Once this is done, all future pushed commits and pull requests will be tested using `build2` CI.

For various reasons such as intermittent network issues, GitHub dropping requests for unknown reasons, etc., a CI might get "stuck" with one or more builds in the queued or building state. Note that in this case, GitHub will not allow you to re-request the CI since it requires all the checks to be completed before that can be done. However, the `CONCLUSION` check contains a link that allows you to force rebuild even if some builds are still outstanding. Note that you should use this mechanism only when you are reasonably sure the CI is stuck in order not to waster CI resources.

While you can stop here, it is strongly recommended to also enable a branch protection rule that takes into account the configured CI. As discussed in the previous section, GitHub CI model has a number of limitations and without the branch protection you may, for example, make a decision to merge a PR based on the stale CI results.

There are two ways to enable the necessary branch protection: using the classic branch protection rule or with the new rulesets. Both of these methods should produce the same result and are discussed in the following two sections.

Note, however, that before you can proceed to enabling branch protection, you need to trigger at least one CI job (for example, by pushing a commit). Failed, that, the `CONCLUSION` check that we will use as the required check will not yet be known in this repository.

## 5.2.1 Adding classic branch protection rule

Go to the repository settings and open the "Branches" tab. There click on the "Add classic branch protection rule" (or edit an existing rule if you already have one for the branch you wish to protect).

In the "Branch name pattern" specify the branch you would like to protect. Usually you protect branches that should only contain successfully checked commits. So normally at least `master/main`.

While you can enable any other protection rules, the one that is pertinent to our problem is "Require status checks to pass before merging". Enable it and then also enable the "Require branches to be up to date before merging" sub-rule. Finally, in the search field type `CONCLUSION` and select it as a required check. Click "Create" (or "Save").

A note on the "Do not allow bypassing the above settings" rule: if you enable it, then repository administrators won't be able to push any commits to the protected branch that haven't been successfully checked. In other words, with this rule enabled, the only way to push a commit – even for repository administrators – would be to first push it to an unprotected branch, wait for the CI to complete, and then, if successful, push it to the protected branch.

## 5.2.2 Adding branch ruleset

Go to the repository settings and open the "Rules/Rulesets" tab. There click on the "New ruleset/New branch ruleset" (or edit an existing ruleset if you already have one for the branch you wish to protect).

In the "Ruleset Name" specify an appropriate name, for example `build2 CI`.

In the "Enforcement status" select "Active".

In the "Target branches" specify the branch you would like to protect. Usually you protect branches that should only contain successfully checked commits. So normally at least `master/main`. If that's your default branch, then selecting "Include default branch" should do the trick.

While you can enable any other protection rules, the one that is pertinent to our problem is "Require status checks to pass". Enable it and then also enable the "Require branches to be up to date before merging" sub-rule. Finally, click on "Add checks" and in the search field type `CONCLUSION` and select it as a required check. Click "Create" (or "Save changes").

A note on the "Bypass list": if you don't add the "Repository admin" role to this list, then repository administrators won't be able to push any commits to the protected branch that haven't been successfully checked. In other words, without this bypass, the only way to push a commit – even for repository administrators – would be to first push it to an unprotected branch, wait for the CI to complete, and then, if successful, push it to the protected branch.