Managing access to other repositories within your codespace

In this article

You can manage the repositories that GitHub Codespaces can access.

Overview

By default, your codespace is assigned a token scoped with `read` permission or `read` and `write` permission to the repository from which it was created. The scope of this token changes automatically in the following circumstances.

- If you create a codespace for a repository to which you only have read access, then make a commit in the codespace or push a new branch, GitHub Codespaces automatically links your codespace to a new or existing fork of the repository and updates the token to have `read` and `write` permission to the fork. For more information, see "Using source control in your codespace."
- If you create a codespace from a template, then publish the codespace to a new repository, GitHub Codespaces updates the token to have `read` and `write` permission to the new repository. For more information, see "Creating a codespace from a template."

For more information, see "Security in GitHub Codespaces."

If your project needs additional permissions for other repositories, you can configure this in the `devcontainer.json` file, as described in "Setting additional repository permissions" later in this article. When permissions are listed in the `devcontainer.json` file, you will be prompted to review and authorize the additional permissions as part of codespace creation for that repository. Once you've authorized the listed permissions, GitHub Codespaces will remember your choice and will not prompt you for authorization unless the permissions in the `devcontainer.json` file change.

Note: Updating the permissions in the `devcontainer.json` file does not change the permissions of existing codespaces. If you need additional permissions in an existing codespace, see "Troubleshooting authentication to a repository."

Creating codespaces with custom permissions

To create a codespace with custom permissions, you must use one of the following:

- The GitHub web UI
- GitHub CLI 2.5.2 or later
- GitHub Codespaces Visual Studio Code extension 1.5.3 or later

Setting additional repository permissions

You configure repository permissions for GitHub Codespaces in a `devcontainer.json` file. Any custom permissions you add or change will only apply to new codespaces created after your changes have been committed to the repository. If you add or change permissions from within a codespace those permissions will not apply to the current codespace, even if you rebuild the codespace.

1. If your repository does not already contain a `devcontainer.json` file, add one now. For more information, see "Adding a dev container configuration to your repository."
2. Edit the `devcontainer.json` file, adding the repository name and permissions needed to the `repositories` object:

JSON

```
{
  "customizations": {
    "codespaces": {
      "repositories": {
        "my_org/my_repo": {
          "permissions": {
            "issues": "write"
          }
        }
      }
    }
  }
}
```

Note: You can only reference repositories that belong to the same personal account or organization as the repository you are currently working in.

You can grant as many or as few of the following permissions for each repository listed:

- `actions` - read / write
- `checks` - read / write
- `contents` - read / write
- `deployments` - read / write
- `discussions` - read / write
- `issues` - read / write
- `packages` - read
- `pages` - read / write
- `pull_requests` - read / write
- `repository_projects` - read / write
- `statuses` - read / write
- `workflows` - write

To set a permission for a repository in an organization, you must explicitly add that repository name in the `repositories` object.

```
{
```

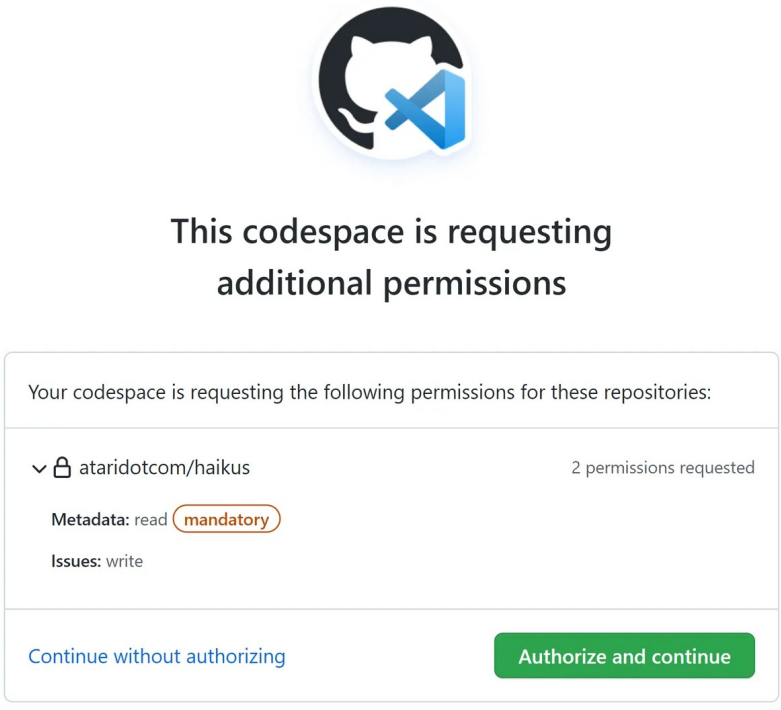
```
  "customizations": {
    "codespaces": {
      "repositories": {
        "my_org/my_repo": {
          "permissions": {
            "issues": "write"
          }
        }
      }
    }
  }
}
```

To set all permissions for a given repository, use `"permissions": "read-all"` or `"permissions": "write-all"` in the repository object.

```
{
  "customizations": {
    "codespaces": {
      "repositories": {
        "my_org/my_repo": {
          "permissions": "write-all"
        }
      }
    }
  }
}
```

Authorizing requested permissions

If additional repository permissions are defined in the `devcontainer.json` file, you will be prompted to review and optionally authorize the permissions when you create a codespace or a prebuild configuration for this repository. When you authorize permissions for a repository, GitHub Codespaces will not re-prompt you unless the set of requested permissions has changed for the repository.



You should only authorize permissions for repositories you know and trust. If you don't

trust the set of requested permissions, click **Continue without authorizing** to create the codespace with the base set of permissions. Rejecting additional permissions may impact the functionality of your project within the codespace as the codespace will only have access to the repository from which it was created.

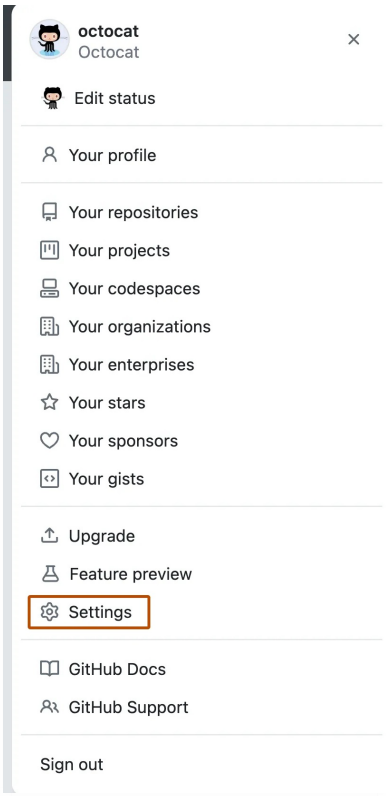
You can only authorize permissions that your personal account already possesses. If a codespace requests permissions for repositories that you don't currently have access to, contact an owner or admin of the repository to obtain sufficient access and then try to create a codespace again.

Access and security

Deprecation note: The access and security setting described below is now deprecated and is documented here for reference only. To enable expanded access to other repositories, add the requested permissions to your dev container definition for your codespace, as described above.

When you enable access and security for a repository owned by your personal account, any codespaces that are created for that repository will have read permissions to all other repositories you own. If you want to restrict the repositories a codespace can access, you can limit to it to either the repository the codespace was opened for or specific repositories. You should only enable access and security for repositories you trust.

1. In the upper-right corner of any page, click your profile photo, then click **Settings**.



2. In the "Code, planning, and automation" section of the sidebar, click **Codespaces**.
3. Under "Access and security," select the setting you want for your personal account:
   - **Disabled** - Limit access of your personal codespaces to the repository they were created from.
   - **All repositories** - All of your personal codespaces can access other repositories you own.

- **Selected repositories** - Personal codespaces created from specific repositories can access other repositories you own.

4. If you chose "Selected repositories", select the "Select repositories" dropdown menu, then click a repository to allow the repository's codespaces to access other repositories you own. Repeat this step for all repositories whose codespaces you want to access other repositories you own.