

Configuring a package's access control and visibility

In this article

- About inheritance of access permissions
- About setting visibility and access permissions for packages
- Configuring access to packages for your personal account
- Configuring access to packages for an organization
- Selecting whether a package inherits permissions from a repository
- Ensuring workflow access to your package
- Configuring visibility of packages for your personal account
- Package creation visibility for organization members
- Configuring visibility of packages for an organization

Choose who has read, write, or admin access to your package and the visibility of your packages on GitHub.

Note: Container registry is currently in beta for GitHub Enterprise Server and subject to change.

Both GitHub Packages and subdomain isolation must be enabled to use Container registry. For more information, see "[Working with the Container registry](#)."

A package can inherit its visibility and access permissions from a repository, or, for registries that support granular permissions, you can set the visibility and permissions of the package separately from a repository.

For the list of registries that support granular permissions, and for more information about permissions for packages, packages-related scopes for PATs, or managing permissions for your GitHub Actions workflows, see "[About permissions for GitHub Packages](#)."

About inheritance of access permissions

In registries that support granular permissions, packages are scoped to a personal account or organization. In these registries, you can publish a package without linking the package to a repository, then determine who can access the package by setting access permissions and visibility in the package's settings.

You can choose to have a package inherit the access permissions of a linked repository. For more information, see "[Selecting whether a package inherits permissions from a repository](#)" below.

If you publish a package in a registry that only supports repository-scoped permissions, the package is always linked to a repository, and always inherits the permissions of the linked repository.

About setting visibility and access permissions for

packages

If a package belongs to a registry that supports granular permissions, anyone with admin permissions to the package can set the package to private or public, and can grant access permissions for the package that are separate from the permissions set at the organization and repository levels. For the list of registries that support granular permissions, see "[About permissions for GitHub Packages](#)."

In most registries, to pull a package, you must authenticate with a personal access token or `GITHUB_TOKEN`, regardless of whether the package is public or private. However, in the Container registry, public packages allow anonymous access and can be pulled without authentication or signing in via the CLI.

When you publish a package, you automatically get admin permissions to the package. If you publish a package to an organization, anyone with the `owner` role in the organization also gets admin permissions to the package.

For packages scoped to a personal account, you can give any person an access role. For packages scoped to an organization, you can give any person or team in the organization an access role.

If you are using a GitHub Actions workflow to manage your packages, you can grant an access role to the repository the workflow is stored in through the **Actions access** menu option. For more information, see "[Configuring a package's access control and visibility](#)."


Permission	Access description
Read	Can download package. Can read package metadata.
Write	Can upload and download this package. Can read and write package metadata.
Admin	Can upload, download, delete, and manage this package. Can read and write package metadata. Can grant package permissions.

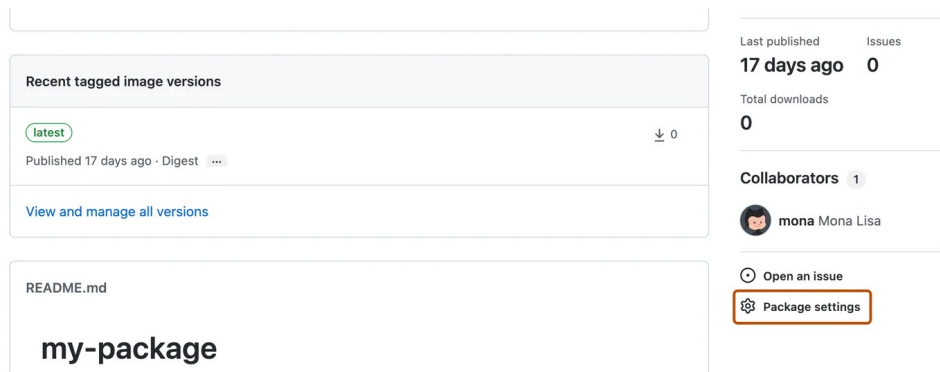
Note: The ability for GitHub Actions workflows to delete and restore packages using the REST API is currently in public beta and subject to change.

Configuring access to packages for your personal account

If you have admin permissions to a package that's scoped to a personal account, you can assign read, write, or admin roles to other users. For more information about these permission roles, see "[Visibility and access permissions for packages](#)."

If your package is private or internal and scoped to an organization, then you can only give access to other organization members or teams.

- 1 Search for and then click the name of the package that you want to manage.
- 2 On your package's landing page, on the right-hand side, click  **Package settings**.



- 3 Under "Manage access" or "Inherited access", click **Invite teams or people** and enter the name, username, or email of the person you want to give access. Teams cannot be given access to a package that is scoped to a personal account.
- 4 Next to the username or team name, use the **Role** drop-down menu to select a desired permission level.

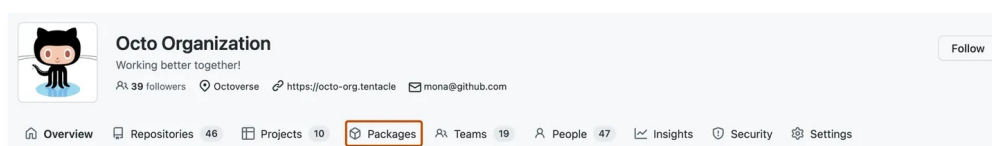
The selected users will automatically be given access and don't need to accept an invitation first.

Configuring access to packages for an organization [🔗](#)

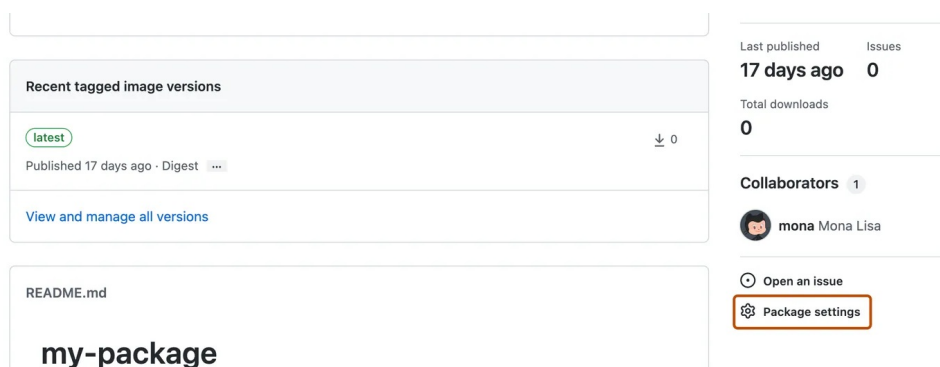
If you have admin permissions to a package that is scoped to an organization, you can assign read, write, or admin roles to other users and teams. For more information about these permission roles, see "[Visibility and access permissions for packages](#)."

If your package is private or internal and scoped to an organization, then you can only give access to other organization members or teams.

- 1 On GitHub, navigate to the main page of your organization.
- 2 Under your organization name, click the **Packages** tab.



- 3 Search for and then click the name of the package that you want to manage.
- 4 On your package's landing page, on the right-hand side, click **Package settings**.



- 5 Under "Manage access" or "Inherited access", click **Invite teams or people** and

enter the name, username, or email of the person you want to give access. You can also enter a team name from the organization to give all team members access.

- 6 Next to the username or team name, use the **Role** drop-down menu to select a desired permission level.

The selected users or teams will automatically be given access and don't need to accept an invitation first.

Selecting whether a package inherits permissions from a repository [↗](#)

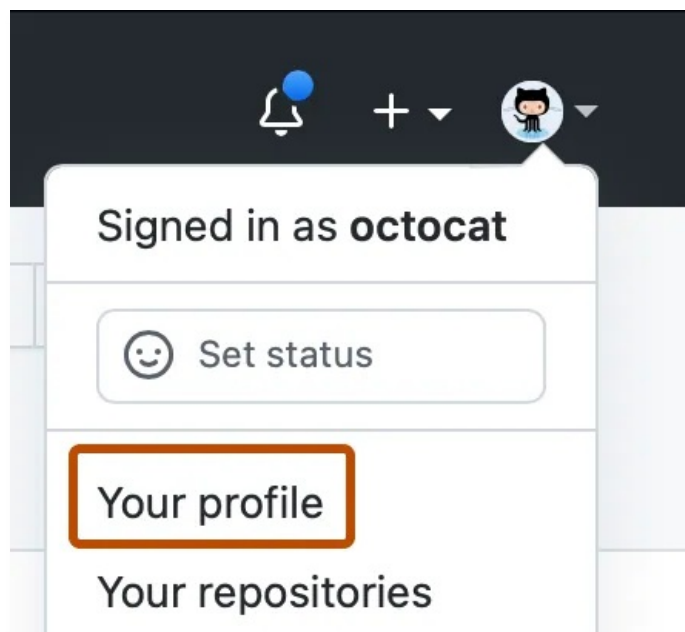
If you link a package to a repository, you can choose whether or not the package inherits the access permissions of the linked repository. We recommend you let packages inherit their permissions from a repository, because this simplifies the process of managing access to a package.

When a package inherits permissions from a repository, to grant or remove access to your package, you must configure the permissions of the linked repository.

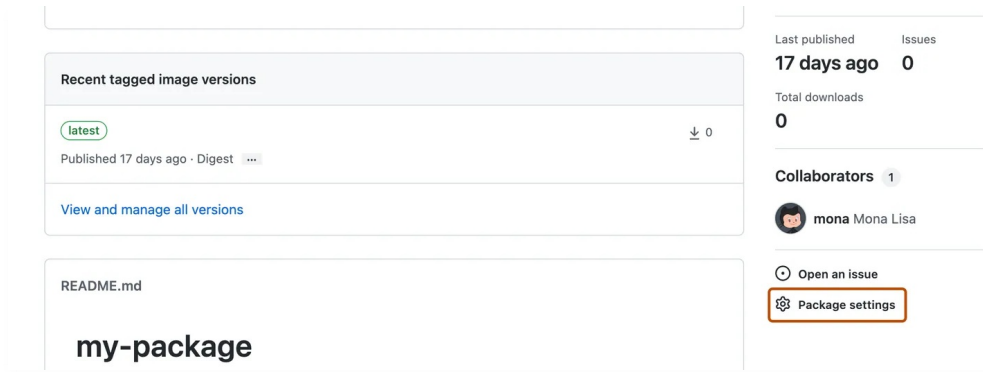
Note: If you change how a package gets its access permissions, any existing permissions for the package are overwritten.

Selecting the inheritance setting for packages scoped to your personal account [↗](#)

- 1 On GitHub, navigate to the main page of your personal account.
- 2 In the top right corner of GitHub Enterprise Server, click your profile photo, then click **Your profile**.




- 3 On your profile page, in the header, click the **Packages** tab.
- 4 Search for and then click the name of the package that you want to manage.
- 5 On your package's landing page, on the right-hand side, click **Package settings**.

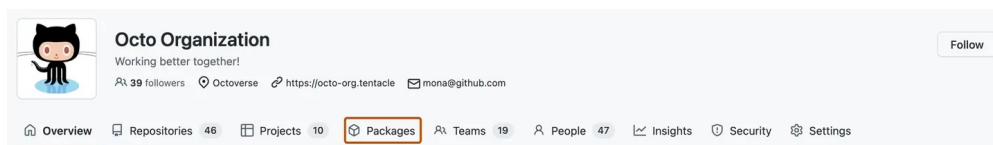



- 6 To choose whether a package inherits access permissions from the linked repository, under "Manage access" or "Inherited access", select or deselect **Inherit access from repository (recommended)**.

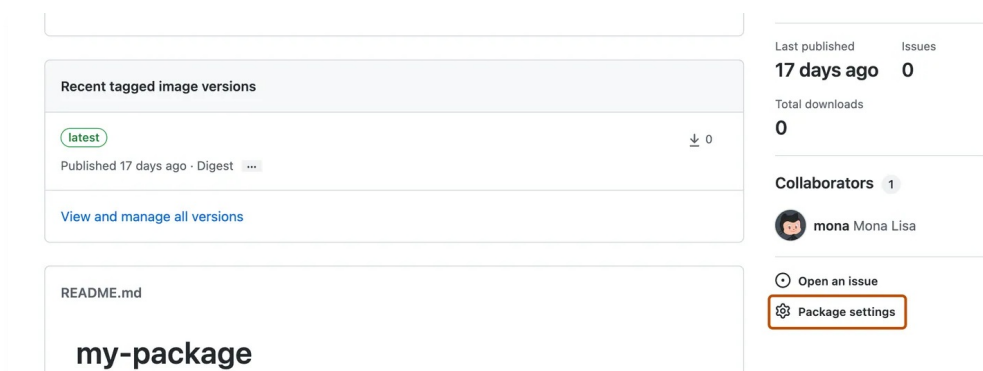
Note: The name of this section changes depending on whether the package already inherits its permissions from a repository.

Selecting the inheritance setting for packages scoped to an organization

- 1 On GitHub, navigate to the main page of your organization.
- 2 Under your organization name, click the  **Packages** tab.



- 3 Search for and then click the name of the package that you want to manage.
- 4 On your package's landing page, on the right-hand side, click  **Package settings**.



- 5 To choose whether a package inherits access permissions from the linked repository, under "Manage access" or "Inherited access", select or deselect **Inherit access from repository (recommended)**.

Note: The name of this section changes depending on whether the package already inherits its permissions from a repository.

Ensuring workflow access to your package


For packages scoped to a personal account or an organization, to ensure that a GitHub Actions workflow has access to your package, you must give explicit access to the repository where the workflow is stored.

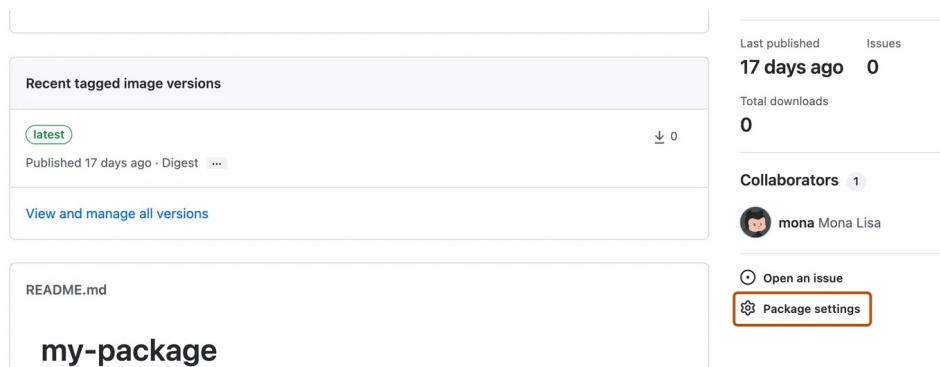
The specified repository does not need to be the repository where the source code for the package is kept. You can give multiple repositories workflow access to a package.

Notes:

- Syncing your package with a repository through the **Actions access** menu option is different than connecting your package to a repository. For more information about linking a repository to your package, see "[Connecting a repository to a package](#)."
- You can choose to limit permissions to workflow jobs using the `permissions` key and `packages` scope. For more information, see "[Assigning permissions to jobs](#)."

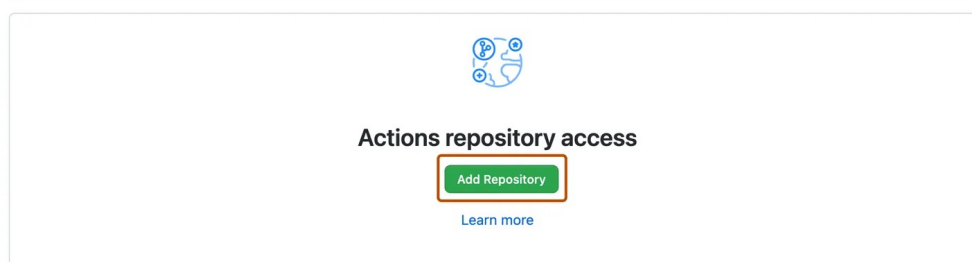
GitHub Actions access for packages scoped to personal accounts

- 1 Search for and then click the name of the package that you want to manage.
- 2 On your package's landing page, on the right-hand side, click  **Package settings**.



- 3 In the left sidebar, click **Actions access**.
- 4 To ensure your workflow has access to your package, you must add the repository where the workflow is stored. Click **Add repository** and search for the repository you want to add.


Manage Actions access

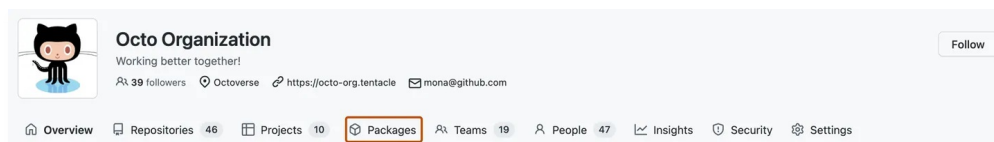



- 5 Use the **Role** drop-down menu to select the default access level that you'd like the repository to have to your package.

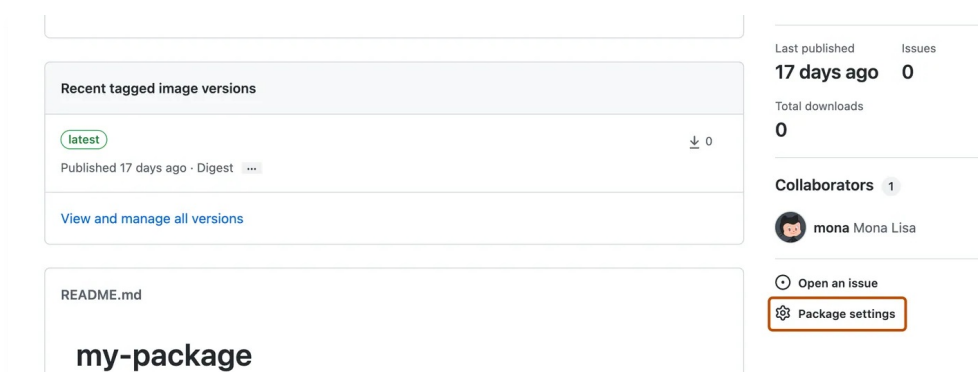
To further customize access to your package, see "[Configuring access to packages for your personal account](#)."

GitHub Actions access for packages scoped to organizations

- 1 On GitHub, navigate to the main page of your organization.
- 2 Under your organization name, click the  **Packages** tab.

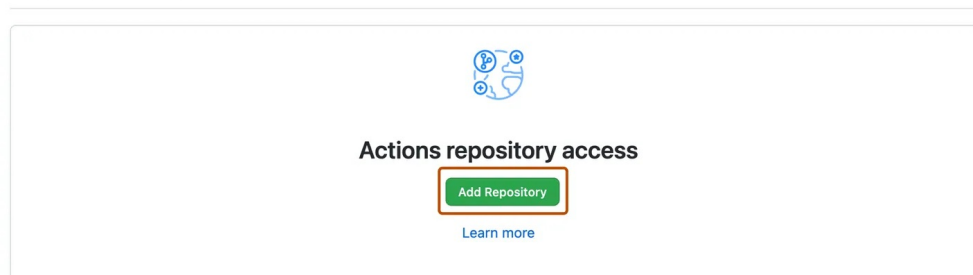


- 3 Search for and then click the name of the package that you want to manage.
- 4 On your package's landing page, on the right-hand side, click  **Package settings**.



- 5 In the left sidebar, click **Actions access**.
- 6 Click **Add repository** and search for the repository you want to add.

Manage Actions access




- 7 Use the **Role** drop-down menu to select the default access level that you'd like the repository to have to your package.

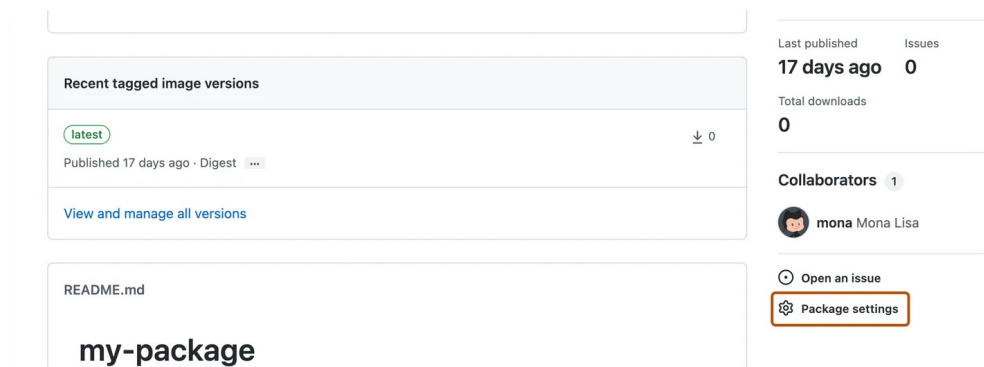
To further customize access to your package, see "[Configuring access to packages for an organization](#)."

Configuring visibility of packages for your personal account

When you first publish a package that is scoped to your personal account, the default visibility is private and only you can see the package. You can modify a private or public

package's access by changing the access settings. Once you make your package public, you cannot make your package private again.

- 1 Search for and then click the name of the package that you want to manage.
- 2 On your package's landing page, on the right-hand side, click  **Package settings**.



- 3 At the bottom of the page, under "Danger Zone", click **Change visibility**.

- 4 Select a visibility setting:

- To make the package visible to anyone, select **Public**.

Warning: Once you make a package public, you cannot make it private again.

- To make the package visible to a custom selection of people, select **Private**.

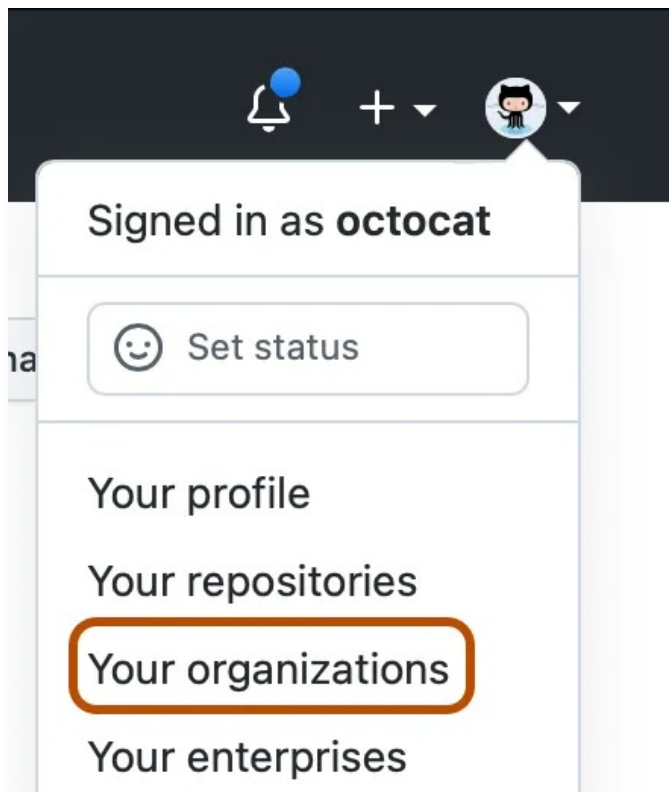
- 5 To confirm, type the name of the package, then click **I understand the consequences, change package visibility**.

Package creation visibility for organization members



For registries that support granular permissions, you can choose the visibility of packages that organization members can publish by default. For the list of these registries, see "[About permissions for GitHub Packages](#)."


- 1 In the top right corner of GitHub Enterprise Server, click your profile photo, then click **Your organizations**.

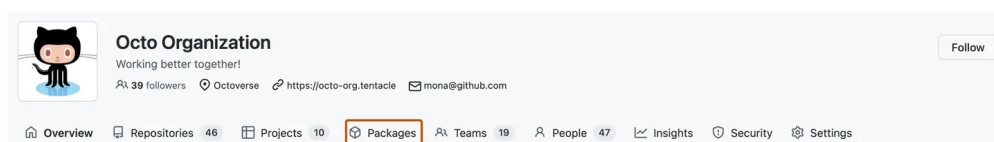



- 2 Next to the organization, click **Settings**.
- 3 On the left, click **Packages**.
- 4 Under "Package Creation", choose whether you want to enable the creation of public, private, or internal packages.
 - To enable organization members to create public packages, click **Public**.
 - To enable organization members to create private packages that are only visible to other organization members, click **Private**. You can further customize the visibility of private packages.
 - To enable organization members to create internal packages that are visible to all organization members, click **Internal**. If the organization belongs to an enterprise, the packages will be visible to all enterprise members.

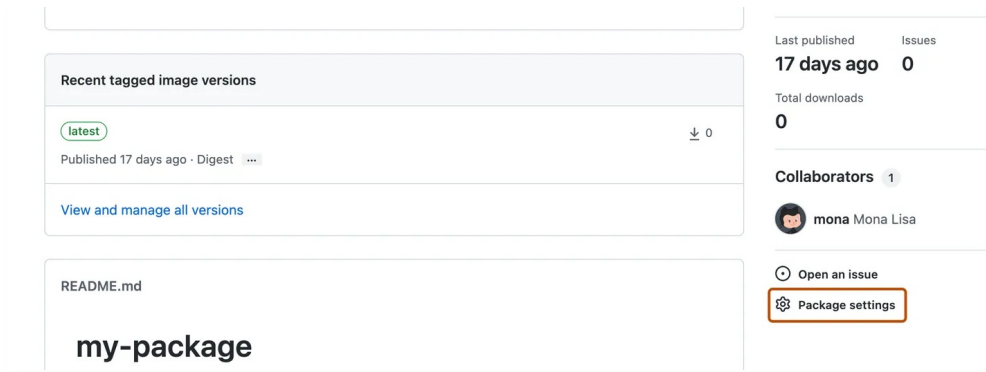
Configuring visibility of packages for an organization [↗](#)

When you first publish a package, the default visibility is private and only you can see the package. You can grant users or teams different access roles for your package through the access settings. Once you make your package public, you cannot make your package private again.

- 1 On GitHub, navigate to the main page of your organization.
- 2 Under your organization name, click the  **Packages** tab.



- 3 Search for and then click the name of the package that you want to manage.
- 4 On your package's landing page, on the right-hand side, click  **Package settings**.



- 5 At the bottom of the page, under "Danger Zone", click **Change visibility** and choose a visibility setting:
 - To make the package visible to anyone, click **Public**.

Warning: Once you make a package public, you cannot make it private again.

- To make the package visible to a custom selection of people in your organization, click **Private**.
- To make the package visible to all organization members, click **Internal**. If the organization belongs to an enterprise, the packages will be visible to all enterprise members.

Legal