REST API / Actions / Permissions

GitHub Docs





The REST API is now versioned. For more information, see "About API versioning."

GitHub Actions Permissions

Use the REST API to interact with permissions for GitHub Actions.

About permissions for GitHub Actions &

You can use the REST API to set permissions for the enterprises, organizations and repositories that are allowed to run GitHub Actions, and the actions and reusable workflows that are allowed to run. For more information, see "<u>Usage limits</u>, billing, and administration."

Get GitHub Actions permissions for an enterprise *P*

Gets the GitHub Actions permissions policy for organizations and allowed actions and reusable workflows in an enterprise.

You must authenticate using an access token with the admin:enterprise scope to use this endpoint.

Parameters for "Get GitHub Actions permissions for an enterprise"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

enterprise string Required

The slug version of the enterprise name. You can also substitute this value with the enterprise id.

HTTP response status codes for "Get GitHub Actions permissions for an enterprise"

Status code Description

200 OK

Code samples for "Get GitHub Actions permissions for an enterprise"



Response

```
Example response Response schema

Status: 200

{ "enabled_organizations": "all", "allowed_actions": "selected", "selected_actions_url": "https://api.github.com/enterprises/2/actions/permissions/selected-actions" }
```

Set GitHub Actions permissions for an enterprise &

Sets the GitHub Actions permissions policy for organizations and allowed actions and reusable workflows in an enterprise.

You must authenticate using an access token with the admin:enterprise scope to use this endpoint.

Parameters for "Set GitHub Actions permissions for an enterprise"

Headers

```
accept string
Setting to application/vnd.github+json is recommended.
```

Path parameters

```
enterprise string Required
```

The slug version of the enterprise name. You can also substitute this value with the enterprise id.

Body parameters

```
enabled_organizations string Required
```

The policy that controls the organizations in the enterprise that are allowed to run GitHub Actions.

Can be one of: all, none, selected

```
allowed_actions string
```

The permissions policy that controls the actions and reusable workflows that are allowed to run.

Can be one of: all, local_only, selected

HTTP response status codes for "Set GitHub Actions permissions for an enterprise"

Status code Description

No Content

Code samples for "Set GitHub Actions permissions for an enterprise"



Response

Status: 204

List selected organizations enabled for GitHub Actions in an enterprise



Lists the organizations that are selected to have GitHub Actions enabled in an enterprise. To use this endpoint, the enterprise permission policy for <code>enabled_organizations</code> must be configured to <code>selected</code>. For more information, see "Set GitHub Actions permissions for an enterprise."

You must authenticate using an access token with the admin:enterprise scope to use this endpoint.

Parameters for "List selected organizations enabled for GitHub Actions in an enterprise"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

enterprise string Required

The slug version of the enterprise name. You can also substitute this value with the enterprise id.

Query parameters

per_page integer

The number of results per page (max 100).

Default: 30

page integer

Page number of the results to fetch.

Default: 1

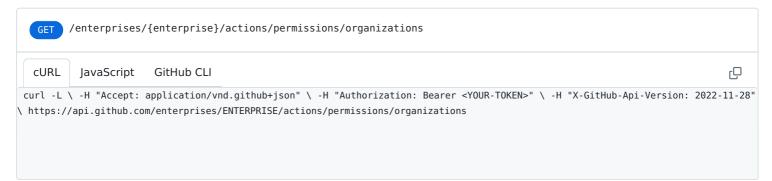
DC:44:0 1

HTTP response status codes for "List selected organizations enabled for GitHub Actions in an enterprise"

Status code Description

200 OK

Code samples for "List selected organizations enabled for GitHub Actions in an enterprise"



Response

```
Example response Response schema

Status: 200

{ "total_count": 1, "organizations": [ { "login": "octocat", "id": 161335, "node_id": "MDEwOlJlcG9zaXRvcnkxMjk2MjY5", "url": "https://api.github.com/orgs/octo-org", "repos_url": "https://api.github.com/orgs/octo-org/repos", "events_url": "https://api.github.com/orgs/octo-org/hooks", "issues_url": "https://api.github.com/orgs/octo-org/hooks", "issues_url": "https://api.github.com/orgs/octo-org/members{/member}", "public_members_url": "https://api.github.com/orgs/octo-org/members{/member}", "avatar_url": "https://github.com/images/error/octocat_happy.gif", "description": "A great organization" } ] }
```

Set selected organizations enabled for GitHub Actions in an enterprise



Replaces the list of selected organizations that are enabled for GitHub Actions in an enterprise. To use this endpoint, the enterprise permission policy for enabled_organizations must be configured to selected. For more information, see "Set GitHub Actions permissions for an enterprise."

You must authenticate using an access token with the admin:enterprise scope to use this endpoint.

Parameters for "Set selected organizations enabled for GitHub Actions in an enterprise"

Headers

accept string
Setting to application/vnd.github+json is recommended.

Path parameters

enterprise string Required

The slug version of the enterprise name. You can also substitute this value with the enterprise id.

the diag relation of the enterprise name, for can also bassactate and raide man the enterprise far

Body parameters

selected_organization_ids array of integers Required

List of organization IDs to enable for GitHub Actions.

HTTP response status codes for "Set selected organizations enabled for GitHub Actions in an enterprise"

Status code Description

204 No Content

Code samples for "Set selected organizations enabled for GitHub Actions in an enterprise"



Response

Status: 204

Enable a selected organization for GitHub Actions in an enterprise &

Adds an organization to the list of selected organizations that are enabled for GitHub Actions in an enterprise. To use this endpoint, the enterprise permission policy for <code>enabled_organizations</code> must be configured to <code>selected</code>. For more information, see "Set GitHub Actions permissions for an enterprise."

You must authenticate using an access token with the admin:enterprise scope to use this endpoint.

Parameters for "Enable a selected organization for GitHub Actions in an enterprise"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

enterprise string Required

The slug version of the enterprise name. You can also substitute this value with the enterprise id.

ora id integer Required

U. g_za meeger meganea

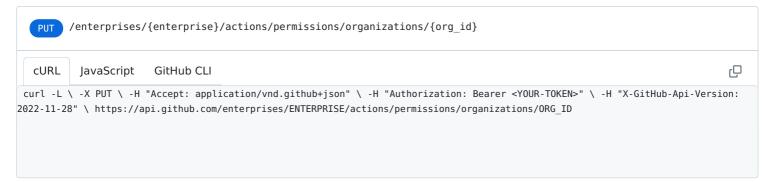
The unique identifier of the organization.

HTTP response status codes for "Enable a selected organization for GitHub Actions in an enterprise"

Status code Description

204 No Content

Code samples for "Enable a selected organization for GitHub Actions in an enterprise"



Response

Status: 204

Disable a selected organization for GitHub Actions in an enterprise &

Removes an organization from the list of selected organizations that are enabled for GitHub Actions in an enterprise. To use this endpoint, the enterprise permission policy for <code>enabled_organizations</code> must be configured to <code>selected</code>. For more information, see "Set GitHub Actions permissions for an enterprise."

You must authenticate using an access token with the admin:enterprise scope to use this endpoint.

Parameters for "Disable a selected organization for GitHub Actions in an enterprise"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

enterprise string Required

The slug version of the enterprise name. You can also substitute this value with the enterprise id.

org_id integer Required

The unique identifier of the organization.

HTTP response status codes for "Disable a selected organization for GitHub Actions in an enterprise"

Status code	Description
204	No Content

Code samples for "Disable a selected organization for GitHub Actions in an enterprise"



Response

Status: 204

Get allowed actions and reusable workflows for an enterprise &

Gets the selected actions and reusable workflows that are allowed in an enterprise. To use this endpoint, the enterprise permission policy for allowed_actions must be configured to selected. For more information, see "Set GitHub Actions permissions for an enterprise."

You must authenticate using an access token with the admin:enterprise scope to use this endpoint.

Parameters for "Get allowed actions and reusable workflows for an enterprise"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

enterprise string Required

The slug version of the enterprise name. You can also substitute this value with the enterprise id.

HTTP response status codes for "Get allowed actions and reusable workflows for an enterprise"

Status code Description

200 OK

Code samples for "Get allowed actions and reusable workflows for an enterprise"

GET /enterprises/{enterprise}/actions/permissions/selected-actions

cURL JavaScript GitHub CLI

curl -L \ -H "Accept: application/vnd.github+json" \ -H "Authorization: Bearer <YOUR-TOKEN>" \ -H "X-GitHub-Api-Version: 2022-11-28" \ https://api.github.com/enterprises/ENTERPRISE/actions/permissions/selected-actions

Response

```
Example response Response schema

Status: 200

{ "github_owned_allowed": true, "verified_allowed": false, "patterns_allowed": [ "monalisa/octocat@*", "docker/*" ] }
```

Set allowed actions and reusable workflows for an enterprise *∂*

Sets the actions and reusable workflows that are allowed in an enterprise. To use this endpoint, the enterprise permission policy for allowed_actions must be configured to selected. For more information, see "Set GitHub Actions permissions for an enterprise."

You must authenticate using an access token with the admin:enterprise scope to use this endpoint.

Parameters for "Set allowed actions and reusable workflows for an enterprise"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

enterprise string Required

The slug version of the enterprise name. You can also substitute this value with the enterprise id.

Body parameters

github_owned_allowed boolean

Whether GitHub-owned actions are allowed. For example, this includes the actions in the actions organization.

verified_allowed boolean

Whether actions from GitHub Marketplace verified creators are allowed. Set to true to allow all actions by GitHub Marketplace verified creators.

patterns_allowed array of strings

Specifies a list of string-matching patterns to allow specific action(s) and reusable workflow(s). Wildcards, tags, and SHAs are allowed.

HTTP response status codes for "Set allowed actions and reusable workflows for an enterprise"

Status code Description

204 No Content

Code samples for "Set allowed actions and reusable workflows for an enterprise"

/ venterprises/{enterprise}/actions/permissions/selected-actions

| CURL | JavaScript | GitHub CLI | Curl -L \ -X PUT \ -H "Accept: application/vnd.github+json" \ -H "Authorization: Bearer <YOUR-TOKEN>" \ -H "X-GitHub-Api-Version: 2022-11-28" \ https://api.github.com/enterprises/ENTERPRISE/actions/permissions/selected-actions \ -d '{"github_owned_allowed":true,"verified_allowed":false, "patterns_allowed":["monalisa/octocat@*","docker/*"]}'

Response

Status: 204

Get default workflow permissions for an enterprise &

Gets the default workflow permissions granted to the GITHUB_TOKEN when running workflows in an enterprise, as well as whether GitHub Actions can submit approving pull request reviews. For more information, see "Enforcing a policy for workflow permissions in your enterprise."

You must authenticate using an access token with the admin:enterprise scope to use this endpoint.

Parameters for "Get default workflow permissions for an enterprise"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

enterprise string Required

The slug version of the enterprise name. You can also substitute this value with the enterprise id.

HTTP response status codes for "Get default workflow permissions for an enterprise"

Status code Description

200 Success response

Code samples for "Get default workflow permissions for an enterprise"



Give read-only permission, and allow approving PRs.

```
Example response Response schema

Status: 200

{ "default_workflow_permissions": "read", "can_approve_pull_request_reviews": true }
```

Set default workflow permissions for an enterprise &

Sets the default workflow permissions granted to the GITHUB_TOKEN when running workflows in an enterprise, and sets whether GitHub Actions can submit approving pull request reviews. For more information, see "Enforcing a policy for workflow permissions in your enterprise."

You must authenticate using an access token with the admin:enterprise scope to use this endpoint.

Parameters for "Set default workflow permissions for an enterprise"

Headers

accept string
Setting to application/vnd.github+json is recommended.

Path parameters

enterprise string Required

The slug version of the enterprise name. You can also substitute this value with the enterprise id.

Body parameters

default_workflow_permissions string

The default workflow permissions granted to the GITHUB TOKEN when running workflows.

Can be one of: read , write

can_appi ove_purr_i equesr_i evtems nooiean

Whether GitHub Actions can approve pull requests. Enabling this can be a security risk.

HTTP response status codes for "Set default workflow permissions for an enterprise"

Status code Description

Success response

Code samples for "Set default workflow permissions for an enterprise"



Success response

Status: 204

Get GitHub Actions permissions for an organization &

Works with <u>GitHub Apps</u>

Gets the GitHub Actions permissions policy for repositories and allowed actions and reusable workflows in an organization.

You must authenticate using an access token with the admin:org scope to use this endpoint. GitHub Apps must have the administration organization permission to use this API.

Parameters for "Get GitHub Actions permissions for an organization"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

org string Required

The organization name. The name is not case sensitive.

HTTP response status codes for "Get GitHub Actions permissions for an organization"

Status code Description

200 OK

Code samples for "Get GitHub Actions permissions for an organization"



Response

```
Example response Response schema

Status: 200

{ "enabled_repositories": "all", "allowed_actions": "selected", "selected_actions_url": "https://api.github.com/organizations/42/actions/permissions/selected-actions" }
```

Set GitHub Actions permissions for an organization $\mathscr {P}$

Works with <u>GitHub Apps</u>

Sets the GitHub Actions permissions policy for repositories and allowed actions in an organization.

If the organization belongs to an enterprise that has set restrictive permissions at the enterprise level, such as allowed actions to selected actions, then you cannot override them for the organization.

You must authenticate using an access token with the admin:org scope to use this endpoint. GitHub Apps must have the administration organization permission to use this API.

Parameters for "Set GitHub Actions permissions for an organization"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

org string Required

The organization name. The name is not case sensitive.

Body parameters

enabled_repositories string Required

The policy that controls the repositories in the organization that are allowed to run GitHub Actions.

Can be one of: all, none, selected

```
allowed_actions string
```

The permissions policy that controls the actions and reusable workflows that are allowed to run.

Can be one of: all, local_only, selected

HTTP response status codes for "Set GitHub Actions permissions for an organization"

Status code	Description
204	No Content

Code samples for "Set GitHub Actions permissions for an organization"



Response

Status: 204

List selected repositories enabled for GitHub Actions in an organization $\mathscr {D}$

Works with GitHub Apps

Lists the selected repositories that are enabled for GitHub Actions in an organization. To use this endpoint, the organization permission policy for <code>enabled_repositories</code> must be configured to <code>selected</code>. For more information, see "Set GitHub Actions permissions for an organization."

You must authenticate using an access token with the admin:org scope to use this endpoint. GitHub Apps must have the administration organization permission to use this API.

Parameters for "List selected repositories enabled for GitHub Actions in an organization"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

org string Required

The organization name. The name is not case sensitive.

Query parameters

per_page integer

The number of results per page (max 100).

Default: 30

page integer

Page number of the results to fetch.

Default: 1

HTTP response status codes for "List selected repositories enabled for GitHub Actions in an organization"

Status code Description

200 OK

Code samples for "List selected repositories enabled for GitHub Actions in an organization"



Response

Example response Response schema

Status: 200

{ "total_count": 1, "repositories": [{ "id": 1296269, "node_id": "MDEwOlJlcG9zaXRvcnkxMjk2MjY5", "name": "Hello-World", "full_name": "octocat/Hello-World", "owner": { "login": "octocat", "id": 1, "node_id": "MDQ6VXNlcjE=", "avatar_url": "https://github.com/images/error/octocat_happy.gif", "gravatar_id": "", "url": "https://api.github.com/users/octocat", "html_url": "https://api.github.com/octocat", "followers_url": "https://api.github.com/users/octocat/following{/other_user}", "gists_url": "https://api.github.com/users/octocat/gists{/gist_id}", "starred_url": "https://api.github.com/users/octocat/starred{/owner}{/repo}", "subscriptions_url": "#ttps://api.github.com/users/octocat/starred{/owner}{/repo}", "subscriptions_url": "#ttps://api.github.com/users/octocat/starred/url": "#ttps://api.github.com/users/octocat/starred/url": "#ttps://api.github.com/users/octocat/starred/url": "#ttps://api.github.com/users/octocat/starred/url": "#ttps://api.github.com/users/octocat/starred/url": "#ttps://api.github.com/users/url": "#ttps://api.github.com/users/url": "#ttps:/

Set selected repositories enabled for GitHub Actions in an organization ${\mathscr O}$

Works with <u>GitHub Apps</u>

Replaces the list of selected repositories that are enabled for GitHub Actions in an organization. To use this endpoint, the organization permission policy for <code>enabled_repositories</code> must be configured to <code>selected</code>. For more information,

see "Set GitHub Actions permissions for an organization."

You must authenticate using an access token with the admin:org scope to use this endpoint. GitHub Apps must have the administration organization permission to use this API.

Parameters for "Set selected repositories enabled for GitHub Actions in an organization"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

org string Required

The organization name. The name is not case sensitive.

Body parameters

selected_repository_ids array of integers Required

List of repository IDs to enable for GitHub Actions.

HTTP response status codes for "Set selected repositories enabled for GitHub Actions in an organization"

Status code Description

204 No Content

Code samples for "Set selected repositories enabled for GitHub Actions in an organization"

CURL JavaScript GitHub CLI

curl -L \ -X PUT \ -H "Accept: application/vnd.github+json" \ -H "Authorization: Bearer <YOUR-TOKEN>" \ -H "X-GitHub-Api-Version: 2022-11-28" \ https://api.github.com/orgs/ORG/actions/permissions/repositories \ -d '{"selected_repository_ids":[32,42]}'

Response

Status: 204

Enable a selected repository for GitHub Actions in an organization @

Works with <u>GitHub Apps</u>

Adds a repository to the list of selected repositories that are enabled for GitHub Actions in an organization. To use this

endpoint, the organization permission policy for enabled_repositories must be must be configured to selected . For more information, see "Set GitHub Actions permissions for an organization."

You must authenticate using an access token with the admin:org scope to use this endpoint. GitHub Apps must have the administration organization permission to use this API.

Parameters for "Enable a selected repository for GitHub Actions in an organization"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

org string Required

The organization name. The name is not case sensitive.

repository_id integer Required

The unique identifier of the repository.

HTTP response status codes for "Enable a selected repository for GitHub Actions in an organization"

Status code Description

No Content

Code samples for "Enable a selected repository for GitHub Actions in an organization"

PUT /orgs/{org}/actions/permissions/repositories/{repository_id}

cURL JavaScript GitHub CLI

curl -L \ -X PUT \ -H "Accept: application/vnd.github+json" \ -H "Authorization: Bearer <YOUR-TOKEN>" \ -H "X-GitHub-Api-Version: 2022-11-28" \ https://api.github.com/orgs/ORG/actions/permissions/repositories/REPOSITORY_ID

Q

Response

Status: 204

Disable a selected repository for GitHub Actions in an organization &

Works with <u>GitHub Apps</u>

Removes a repository from the list of selected repositories that are enabled for GitHub Actions in an organization. To use this endpoint, the organization permission policy for <code>enabled_repositories</code> must be configured to <code>selected</code>. For more information, see "Set GitHub Actions permissions for an organization."

You must authenticate using an access token with the admin:org scope to use this endpoint. GitHub Apps must have the administration organization permission to use this API.

Parameters for "Disable a selected repository for GitHub Actions in an organization"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

org string Required

The organization name. The name is not case sensitive.

repository_id integer Required

The unique identifier of the repository.

HTTP response status codes for "Disable a selected repository for GitHub Actions in an organization"

Status code	Description
204	No Content

Code samples for "Disable a selected repository for GitHub Actions in an organization"

CURL JavaScript GitHub CLI

curl -L \ -X DELETE \ -H "Accept: application/vnd.github+json" \ -H "Authorization: Bearer <YOUR-TOKEN>" \ -H "X-GitHub-Api-Version: 2022-11-28" \ https://api.github.com/orgs/ORG/actions/permissions/repositories/REPOSITORY_ID

Response

Status: 204

Get allowed actions and reusable workflows for an organization &

Works with <u>GitHub Apps</u>

Gets the selected actions and reusable workflows that are allowed in an organization. To use this endpoint, the organization permission policy for allowed_actions must be configured to selected. For more information, see "Set GitHub Actions permissions for an organization."

You must authenticate using an access token with the admin:org scope to use this endpoint. GitHub Apps must have the administration organization permission to use this API.

Parameters for "Get allowed actions and reusable workflows for an organization"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

org string Required

The organization name. The name is not case sensitive.

HTTP response status codes for "Get allowed actions and reusable workflows for an organization"

Status code Description

Code samples for "Get allowed actions and reusable workflows for an organization"

CURL JavaScript GitHub CLI

CURL L\ -H "Accept: application/vnd.github+json" \ -H "Authorization: Bearer <YOUR-TOKEN>" \ -H "X-GitHub-Api-Version: 2022-11-28" \ https://api.github.com/orgs/ORG/actions/permissions/selected-actions

OK

Response

200

Example response Response schema

Status: 200

{ "github_owned_allowed": true, "verified_allowed": false, "patterns_allowed": ["monalisa/octocat@*", "docker/*"] }

Set allowed actions for an organization ∂

Works with GitHub Apps

Sets the actions that are allowed in an organization. To use this endpoint, the organization permission policy for allowed_actions must be configured to selected. For more information, see "Set GitHub Actions permissions for an organization."

If the organization belongs to an enterprise that has selected actions set at the enterprise level, then you cannot override any of the enterprise's allowed actions settings.

To use the patterns_allowed setting for private repositories, the organization must belong to an enterprise. If the organization does not belong to an enterprise, then the patterns_allowed setting only applies to public repositories in the organization.

You must authenticate using an access token with the admin:org scope to use this endpoint. GitHub Apps must have the administration organization permission to use this API.

Parameters for "Set allowed actions for an organization"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

org string Required

The organization name. The name is not case sensitive.

Body parameters

github_owned_allowed boolean

Whether GitHub-owned actions are allowed. For example, this includes the actions in the actions organization.

verified_allowed boolean

Whether actions from GitHub Marketplace verified creators are allowed. Set to true to allow all actions by GitHub Marketplace verified creators.

patterns_allowed array of strings

Specifies a list of string-matching patterns to allow specific action(s) and reusable workflow(s). Wildcards, tags, and SHAs are allowed. For example, monalisa/octocat@*, monalisa/octocat@v2, monalisa/*.

HTTP response status codes for "Set allowed actions for an organization"

Status code Description

No Content

Code samples for "Set allowed actions for an organization"

PUT /orgs/{org}/actions/permissions/selected-actions

cURL JavaScript GitHub CLI

curl -L \ -X PUT \ -H "Accept: application/vnd.github+json" \ -H "Authorization: Bearer <YOUR-TOKEN>" \ -H "X-GitHub-Api-Version: 2022-11-28" \ https://api.github.com/orgs/ORG/actions/permissions/selected-actions \ -d

إي

'{"github_owned_allowed":true,"verified_allowed":false,"patterns_allowed":["monalisa/octocat@*","docker/*"]}'

Response

Status: 204

Get default workflow permissions for an organization &

Works with <u>GitHub Apps</u>

Gets the default workflow permissions granted to the GITHUB_TOKEN when running workflows in an organization, as well as whether GitHub Actions can submit approving pull request reviews. For more information, see "Setting the permissions of the GITHUB_TOKEN for your organization."

You must authenticate using an access token with the admin:org scope to use this endpoint. GitHub Apps must have the administration organization permission to use this API.

Parameters for "Get default workflow permissions for an organization"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

org string Required

The organization name. The name is not case sensitive.

HTTP response status codes for "Get default workflow permissions for an organization"

Status code Description

200

Code samples for "Get default workflow permissions for an organization"

cURL JavaScript GitHub CLI

OK

curl -L \ -H "Accept: application/vnd.github+json" \ -H "Authorization: Bearer <YOUR-TOKEN>" \ -H "X-GitHub-Api-Version: 2022-11-28" \ https://api.github.com/orgs/ORG/actions/permissions/workflow

Give read-only permission, and allow approving PRs.

GET /orgs/{org}/actions/permissions/workflow

Example response Response schema

Status: 200

{ "default_workflow_permissions": "read", "can_approve_pull_request_reviews": true }

Set default workflow permissions for an organization &

Works with <u>GitHub Apps</u>

Sets the default workflow permissions granted to the GITHUB_TOKEN when running workflows in an organization, and sets if GitHub Actions can submit approving pull request reviews. For more information, see "Setting the permissions of the GITHUB TOKEN for your organization."

You must authenticate using an access token with the admin:org scope to use this endpoint. GitHub Apps must have the administration organization permission to use this API.

Parameters for "Set default workflow permissions for an organization"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

org string Required

The organization name. The name is not case sensitive.

Body parameters

default_workflow_permissions string

The default workflow permissions granted to the GITHUB_TOKEN when running workflows.

Can be one of: read , write

can_approve_pull_request_reviews boolean

Whether GitHub Actions can approve pull requests. Enabling this can be a security risk.

HTTP response status codes for "Set default workflow permissions for an organization"

Status code	Description
204	Success response
409	Conflict response when changing a setting is prevented by the owning enterprise

Code samples for "Set default workflow permissions for an organization"



'{"default_workflow_permissions":"read","can_approve_pull_request_reviews":true}'

Success response

Status: 204

Get GitHub Actions permissions for a repository $\mathscr P$

Works with <u>GitHub Apps</u>

Gets the GitHub Actions permissions policy for a repository, including whether GitHub Actions is enabled and the actions and reusable workflows allowed to run in the repository.

You must authenticate using an access token with the repo scope to use this endpoint. GitHub Apps must have the administration repository permission to use this API.

Parameters for "Get GitHub Actions permissions for a repository"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

owner string Required

The account owner of the repository. The name is not case sensitive.

repo string Required

The name of the repository without the .git extension. The name is not case sensitive.

HTTP response status codes for "Get GitHub Actions permissions for a repository"

Status code Description

200 OK

Code samples for "Get GitHub Actions permissions for a repository"



Response

```
Example response Response schema

Status: 200

{ "enabled": true, "allowed_actions": "selected", "selected_actions_url": "https://api.github.com/repositories/42/actions/permissions/selected-actions" }
```

Set GitHub Actions permissions for a repository *P*

Works with <u>GitHub Apps</u>

Sets the GitHub Actions permissions policy for enabling GitHub Actions and allowed actions in the repository.

If the repository belongs to an organization or enterprise that has set restrictive permissions at the organization or enterprise levels, such as allowed actions to selected actions, then you cannot override them for the repository.

You must authenticate using an access token with the repo scope to use this endpoint. GitHub Apps must have the administration repository permission to use this API.

Parameters for "Set GitHub Actions permissions for a repository"

Headers

accept string
Setting to application/vnd.github+json is recommended.

Path parameters

owner string Required

The account owner of the repository. The name is not case sensitive.

repo string Required

The name of the repository without the .git extension. The name is not case sensitive.

Body parameters

enabled boolean Required

Whether GitHub Actions is enabled on the repository.

allowed_actions string

The permissions policy that controls the actions and reusable workflows that are allowed to run.

Can be one of: all, local_only, selected

HTTP response status codes for "Set GitHub Actions permissions for a repository"

Status code Description

204 No Content

Code samples for "Set GitHub Actions permissions for a repository"



Response

Status: 204

Get the level of access for workflows outside of the repository &

Works with GitHub Apps

Gets the level of access that workflows outside of the repository have to actions and reusable workflows in the repository. This endpoint only applies to internal and private repositories. For more information, see "Allowing access to components in a private repository." and "Allowing access to components in an internal repository."

You must authenticate using an access token with the repo scope to use this endpoint. GitHub Apps must have the repository administration permission to use this endpoint.

Parameters for "Get the level of access for workflows outside of the repository"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

owner string Required

The account owner of the repository. The name is not case sensitive.

repo string Required

The name of the repository without the .git extension. The name is not case sensitive.

Status code Description

200 OK

Code samples for "Get the level of access for workflows outside of the repository"



Response

```
Example response Response schema

Status: 200

{ "access_level": "organization" }
```

Set the level of access for workflows outside of the repository $\ensuremath{\mathscr{E}}$

Works with <u>GitHub Apps</u>

Sets the level of access that workflows outside of the repository have to actions and reusable workflows in the repository. This endpoint only applies to internal and private repositories. For more information, see "Allowing access to components in a private repository." and "Allowing access to components in an internal repository."

You must authenticate using an access token with the repo scope to use this endpoint. GitHub Apps must have the repository administration permission to use this endpoint.

Parameters for "Set the level of access for workflows outside of the repository"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

owner string Required

The account owner of the repository. The name is not case sensitive.

repo string Required

The name of the repository without the .git extension. The name is not case sensitive.

Body parameters

access_level string Required

Defines the level of access that workflows outside of the repository have to actions and reusable workflows within the repository.

none means the access is only possible from workflows in this repository. user level access allows sharing across user owned private repos only. organization level access allows sharing across the organization. enterprise level access allows sharing across the enterprise.

Can be one of: none , user , organization , enterprise

HTTP response status codes for "Set the level of access for workflows outside of the repository"

Status code Description

204 No Content

Code samples for "Set the level of access for workflows outside of the repository"



Response

Status: 204

Get allowed actions and reusable workflows for a repository &

Works with <u>GitHub Apps</u>

Gets the settings for selected actions and reusable workflows that are allowed in a repository. To use this endpoint, the repository policy for allowed_actions must be configured to selected. For more information, see "Set GitHub Actions permissions for a repository."

You must authenticate using an access token with the repo scope to use this endpoint. GitHub Apps must have the administration repository permission to use this API.

Parameters for "Get allowed actions and reusable workflows for a repository"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

owner string Required

The account owner of the repository. The name is not case sensitive.

repo string Required

The name of the repository without the .git extension. The name is not case sensitive.

HTTP response status codes for "Get allowed actions and reusable workflows for a repository"

Status code	Description
200	OK

Code samples for "Get allowed actions and reusable workflows for a repository"



Response

```
Example response Response schema

Status: 200

{ "github_owned_allowed": true, "verified_allowed": false, "patterns_allowed": [ "monalisa/octocat@*", "docker/*" ] }
```

Set allowed actions for a repository *∂*

Works with <u>GitHub Apps</u>

Sets the actions that are allowed in a repository. To use this endpoint, the repository permission policy for allowed_actions must be configured to selected. For more information, see "Set GitHub Actions permissions for a repository."

If the repository belongs to an organization or enterprise that has selected actions set at the organization or enterprise levels, then you cannot override any of the allowed actions settings and reusable workflows settings.

To use the patterns_allowed setting for private repositories, the repository must belong to an enterprise. If the repository does not belong to an enterprise, then the patterns_allowed setting only applies to public repositories.

You must authenticate using an access token with the repo scope to use this endpoint. GitHub Apps must have the

administration repository permission to use this API.

Parameters for "Set allowed actions for a repository"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

owner string Required

The account owner of the repository. The name is not case sensitive.

repo string Required

The name of the repository without the .git extension. The name is not case sensitive.

Body parameters

github owned allowed boolean

Whether GitHub-owned actions are allowed. For example, this includes the actions in the actions organization.

verified allowed boolean

Whether actions from GitHub Marketplace verified creators are allowed. Set to true to allow all actions by GitHub Marketplace verified creators.

patterns allowed array of strings

Specifies a list of string-matching patterns to allow specific action(s) and reusable workflow(s). Wildcards, tags, and SHAs are allowed. For example, monalisa/octocat@*, monalisa/octocat@*.

HTTP response status codes for "Set allowed actions for a repository"

Status code Description

204 No Content

Code samples for "Set allowed actions for a repository"

PUT /repos/{owner}/{repo}/actions/permissions/selected-actions

cURL | JavaScript | GitHub CLI

curl -L \ -X PUT \ -H "Accept: application/vnd.github+json" \ -H "Authorization: Bearer <YOUR-TOKEN>" \ -H "X-GitHub-Api-Version: 2022-11-28" \ https://api.github.com/repos/OWNER/REPO/actions/permissions/selected-actions \ -d

ſŪ

'{"github_owned_allowed":true,"verified_allowed":false,"patterns_allowed":["monalisa/octocat@*","docker/*"]}'

Response

Status: 204

Get default workflow permissions for a repository &

Works with <u>GitHub Apps</u>

Gets the default workflow permissions granted to the GITHUB_TOKEN when running workflows in a repository, as well as if GitHub Actions can submit approving pull request reviews. For more information, see "Setting the permissions of the GITHUB_TOKEN for your repository."

You must authenticate using an access token with the repo scope to use this endpoint. GitHub Apps must have the repository administration permission to use this API.

Parameters for "Get default workflow permissions for a repository"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

owner string Required

The account owner of the repository. The name is not case sensitive.

repo string Required

The name of the repository without the <code>.git</code> extension. The name is not case sensitive.

HTTP response status codes for "Get default workflow permissions for a repository"

Status code Description

200 OK

Code samples for "Get default workflow permissions for a repository"

GET /repos/{owner}/{repo}/actions/permissions/workflow

cURL JavaScript GitHub CLI

curl -L \ -H "Accept: application/vnd.github+json" \ -H "Authorization: Bearer <YOUR-TOKEN>" \ -H "X-GitHub-Api-Version: 2022-11-28" \ https://api.github.com/repos/OWNER/REPO/actions/permissions/workflow

Give read-only permission, and allow approving PRs.

Example response Response schema

Status: 200

{ "default_workflow_permissions": "read", "can_approve_pull_request_reviews": true }

Set default workflow permissions for a repository &

Works with <u>GitHub Apps</u>

Sets the default workflow permissions granted to the GITHUB_TOKEN when running workflows in a repository, and sets if GitHub Actions can submit approving pull request reviews. For more information, see "Setting the permissions of the GITHUB TOKEN for your repository."

You must authenticate using an access token with the repo scope to use this endpoint. GitHub Apps must have the repository administration permission to use this API.

Parameters for "Set default workflow permissions for a repository"

Headers

accept string

Setting to application/vnd.github+json is recommended.

Path parameters

owner string Required

The account owner of the repository. The name is not case sensitive.

repo string Required

The name of the repository without the .git extension. The name is not case sensitive.

Body parameters

default_workflow_permissions string

The default workflow permissions granted to the GITHUB_TOKEN when running workflows.

Can be one of: read , write

can_approve_pull_request_reviews boolean

Whether GitHub Actions can approve pull requests. Enabling this can be a security risk.

HTTP response status codes for "Set default workflow permissions for a repository"

Status code	Description
204	Success response
409	Conflict response when changing a setting is prevented by the owning organization or enterprise

Code samples for "Set default workflow permissions for a repository"

PUT /repos/{owner}/{repo}/actions/permissions/workflow

cURL

JavaScript GitHub CLI

Q

2022-11-28" $\$ https://api.github.com/repos/OWNER/REPO/actions/permissions/workflow $\$ -d '{"default_workflow_permissions":"read","can_approve_pull_request_reviews":true}'

Success response

Status: 204

Legal

© 2023 GitHub, Inc. <u>Terms</u> <u>Privacy</u> <u>Status</u> <u>Pricing</u> <u>Expert services</u> <u>Blog</u>