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

Organizations

Use the REST API to interact with organizations.

List organizations

✓ Works with GitHub Apps

Lists all organizations, in the order that they were created on GitHub Enterprise Server.

Note: Pagination is powered exclusively by the `since` parameter. Use the Link header to get the URL for the next page of organizations.

Parameters for "List organizations"

Headers

`accept` string

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

Query parameters

`since` integer

An organization ID. Only return organizations with an ID greater than this ID.

`per_page` integer

The number of results per page (max 100).

Default: `30`

HTTP response status codes for "List organizations"

Status code	Description
`200`	OK
`304`	Not modified

Code samples for "List organizations"

GET /organizations

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" \
http(s)://HOSTNAME/api/v3/organizations
```

Response

Example response   Response schema

```
Status: 200
```

```
 [ { "login": "github", "id": 1, "node_id": "MDEyOk9yZ2FuaXphdGlvbjE=", "url": "https://HOSTNAME/orgs/github", "repos_url":
"https://HOSTNAME/orgs/github/repos", "events_url": "https://HOSTNAME/orgs/github/events", "hooks_url":
"https://HOSTNAME/orgs/github/hooks", "issues_url": "https://HOSTNAME/orgs/github/issues", "members_url":
"https://HOSTNAME/orgs/github/members{/member}", "public_members_url": "https://HOSTNAME/orgs/github/public_members{/member}",
"avatar_url": "https://github.com/images/error/octocat_happy.gif", "description": "A great organization" } ]
```

Get an organization

Works with GitHub Apps

To see many of the organization response values, you need to be an authenticated organization owner with the `admin:org` scope. When the value of `two_factor_requirement_enabled` is `true`, the organization requires all members, billing managers, and outside collaborators to enable two-factor authentication.

GitHub Apps with the `Organization plan` permission can use this endpoint to retrieve information about an organization's GitHub Enterprise Server plan. See "Authenticating with GitHub Apps" for details. For an example response, see 'Response with GitHub Enterprise Server plan information' below."

Parameters for "Get 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 an organization"

Status code	Description
`200`	OK
`404`	Resource not found

Code samples for "Get an organization"

GET /orgs/{org}

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" \
http(s)://HOSTNAME/api/v3/orgs/ORG
```

Response

Example response Response schema

```
Status: 200
```

```
 { "login": "github", "id": 1, "node_id": "MDEyOk9yZ2FuaXphdGlvbjE=", "url": "https://HOSTNAME/orgs/github", "repos_url":
"https://HOSTNAME/orgs/github/repos", "events_url": "https://HOSTNAME/orgs/github/events", "hooks_url":
"https://HOSTNAME/orgs/github/hooks", "issues_url": "https://HOSTNAME/orgs/github/issues", "members_url":
"https://HOSTNAME/orgs/github/members{/member}", "public_members_url": "https://HOSTNAME/orgs/github/public_members{/member}",
"avatar_url": "https://github.com/images/error/octocat_happy.gif", "description": "A great organization", "name": "github", "company":
"GitHub", "blog": "https://github.com/blog", "location": "San Francisco", "email": "octocat@github.com", "twitter_username": "github",
```

Update an organization

✓ Works with GitHub Apps

Parameter Deprecation Notice: GitHub Enterprise Server will replace and discontinue `members_allowed_repository_creation_type` in favor of more granular permissions. The new input parameters are `members_can_create_public_repositories`, `members_can_create_private_repositories` for all organizations and `members_can_create_internal_repositories` for organizations associated with an enterprise account using GitHub Enterprise Cloud or GitHub Enterprise Server 2.20+. For more information, see the blog post.

Enables an authenticated organization owner with the `admin:org` scope or the `repo` scope to update the organization's profile and member privileges.

Parameters for "Update 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

`billing_email` string

Billing email address. This address is not publicized.

`company` string

The company name.

`email` string

The publicly visible email address.

`twitter_username` string

The Twitter username of the company.

`location` string

The location.

`name` string

The shorthand name of the company.

`description` string

The description of the company.

`has_organization_projects` boolean

Whether an organization can use organization projects.

`has_repository_projects` boolean

Whether repositories that belong to the organization can use repository projects.

`default_repository_permission` string

Default permission level members have for organization repositories.

Default: `read`
Can be one of: `read`, `write`, `admin`, `none`

`members_can_create_repositories` boolean

Whether of non-admin organization members can create repositories. **Note:** A parameter can override this parameter. See `members_allowed_repository_creation_type` in this table for details.

Default: `true`

`members_can_create_internal_repositories` boolean

Whether organization members can create internal repositories, which are visible to all enterprise members. You can only allow members to create internal repositories if your organization is associated with an enterprise account using GitHub Enterprise Cloud or GitHub Enterprise Server 2.20+. For more information, see "Restricting repository creation in your organization" in the GitHub Help documentation.

`members_can_create_private_repositories` boolean

Whether organization members can create private repositories, which are visible to organization members with permission. For more information, see "Restricting repository creation in your organization" in the GitHub Help documentation.

`members_can_create_public_repositories` boolean

Whether organization members can create public repositories, which are visible to anyone. For more information, see "Restricting repository creation in your organization" in the GitHub Help documentation.

`members_allowed_repository_creation_type` string

Specifies which types of repositories non-admin organization members can create. **Note:** This parameter is deprecated and will be removed in the future. Its return value ignores internal repositories. Using this parameter overrides values set in `members_can_create_repositories`. See the parameter deprecation notice in the operation description for details.

Can be one of: `all`, `private`, `none`

`members_can_create_pages` boolean

Whether organization members can create GitHub Pages sites. Existing published sites will not be impacted.

Default: `true`

`members_can_fork_private_repositories` boolean

Whether organization members can fork private organization repositories.

Default: `false`

`web_commit_signoff_required` boolean

Whether contributors to organization repositories are required to sign off on commits they make through GitHub's web interface.

Default: `false`

`blog` string

`advanced_security_enabled_for_new_repositories` boolean

Whether GitHub Advanced Security is automatically enabled for new repositories.
To use this parameter, you must have admin permissions for the repository or be an owner or security manager for the organization that owns the repository. For more information, see "Managing security managers in your organization."
You can check which security and analysis features are currently enabled by using a `GET /orgs/{org}` request.

`dependabot_alerts_enabled_for_new_repositories` boolean

Whether Dependabot alerts is automatically enabled for new repositories.
To use this parameter, you must have admin permissions for the repository or be an owner or security manager for the organization that owns the repository. For more information, see "Managing security managers in your organization."
You can check which security and analysis features are currently enabled by using a `GET /orgs/{org}` request.

`dependabot_security_updates_enabled_for_new_repositories` boolean

Whether Dependabot security updates is automatically enabled for new repositories.
To use this parameter, you must have admin permissions for the repository or be an owner or security manager for the organization that owns the repository. For more information, see "Managing security managers in your organization."
You can check which security and analysis features are currently enabled by using a `GET /orgs/{org}` request.

`dependency_graph_enabled_for_new_repositories` boolean

Whether dependency graph is automatically enabled for new repositories.
To use this parameter, you must have admin permissions for the repository or be an owner or security manager for the organization that owns the repository. For more information, see "Managing security managers in your organization."
You can check which security and analysis features are currently enabled by using a `GET /orgs/{org}` request.

`secret_scanning_enabled_for_new_repositories` boolean

Whether secret scanning is automatically enabled for new repositories.
To use this parameter, you must have admin permissions for the repository or be an owner or security manager for the organization that owns the repository. For more information, see "Managing security managers in your organization."
You can check which security and analysis features are currently enabled by using a `GET /orgs/{org}` request.

`secret_scanning_push_protection_enabled_for_new_repositories` boolean

Whether secret scanning push protection is automatically enabled for new repositories.
To use this parameter, you must have admin permissions for the repository or be an owner or security manager for the organization that owns the repository. For more information, see "Managing security managers in your organization."
You can check which security and analysis features are currently enabled by using a `GET /orgs/{org}` request.

`secret_scanning_push_protection_custom_link_enabled` boolean

Whether a custom link is shown to contributors who are blocked from pushing a secret by push protection.

`secret_scanning_push_protection_custom_link` string

If `secret_scanning_push_protection_custom_link_enabled` is true, the URL that will be displayed to contributors who are blocked from pushing a secret.

HTTP response status codes for "Update an organization"

Status code	Description
`200`	OK

`409`	Conflict
`422`	Validation failed

Code samples for "Update an organization"

PATCH /orgs/{org}

cURL JavaScript GitHub CLI

```
 curl -L \ -X PATCH \ -H "Accept: application/vnd.github+json" \ -H "Authorization: Bearer <YOUR-TOKEN>" \ -H "X-GitHub-Api-Version: 2022-
11-28" \ http(s)://HOSTNAME/api/v3/orgs/ORG \ -d
'{"billing_email":"mona@github.com","company":"GitHub","email":"mona@github.com","twitter_username":"github","location":"San
Francisco","name":"github","description":"GitHub, the
company.","default_repository_permission":"read","members_can_create_repositories":true,"members_allowed_repository_creation_type":"all"}'
```

Response

Example response Response schema

```
Status: 200
```

```
 { "login": "github", "id": 1, "node_id": "MDEyOk9yZ2FuaXphdGlvbjE=", "url": "https://HOSTNAME/orgs/github", "repos_url":
"https://HOSTNAME/orgs/github/repos", "events_url": "https://HOSTNAME/orgs/github/events", "hooks_url":
"https://HOSTNAME/orgs/github/hooks", "issues_url": "https://HOSTNAME/orgs/github/issues", "members_url":
"https://HOSTNAME/orgs/github/members{/member}", "public_members_url": "https://HOSTNAME/orgs/github/public_members{/member}",
"avatar_url": "https://github.com/images/error/octocat_happy.gif", "description": "A great organization", "name": "github", "company":
"GitHub", "blog": "https://github.com/blog", "location": "San Francisco", "email": "octocat@github.com", "twitter_username": "github",
```

Delete an organization

✓ Works with GitHub Apps

Deletes an organization and all its repositories.

The organization login will be unavailable for 90 days after deletion.

Please review the Terms of Service regarding account deletion before using this endpoint:

https://docs.github.com/enterprise-server@3.10/site-policy/github-terms/github-terms-of-service

Parameters for "Delete 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 "Delete an organization"

Status code	Description

`202`	Accepted
`403`	Forbidden
`404`	Resource not found

Code samples for "Delete an organization"

DELETE `/orgs/{org}`

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" \ http(s)://HOSTNAME/api/v3/orgs/ORG
```

Accepted

Example response Response schema

```
Status: 202
```

Get the audit log for an organization

✓ Works with GitHub Apps

Gets the audit log for an organization. For more information, see "Reviewing the audit log for your organization."

To use this endpoint, you must be an organization owner, and you must use an access token with the `read:audit_log` scope. GitHub Apps must have the `organization_administration` read permission to use this endpoint.

By default, the response includes up to 30 events from the past three months. Use the `phrase` parameter to filter results and retrieve older events. For example, use the `phrase` parameter with the `created` qualifier to filter events based on when the events occurred. For more information, see "Reviewing the audit log for your organization."

Use pagination to retrieve fewer or more than 30 events. For more information, see "Resources in the REST API."

Parameters for "Get the audit log 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.

Query parameters

`phrase` string

A search phrase. For more information, see Searching the audit log.

`include` string

The event types to include:

- `web` - returns web (non-Git) events.
- `git` - returns Git events.
- `all` - returns both web and Git events.

The default is `web`.

Can be one of: `web`, `git`, `all`

`after` string

A cursor, as given in the Link header. If specified, the query only searches for events after this cursor.

`before` string

A cursor, as given in the Link header. If specified, the query only searches for events before this cursor.

`order` string

The order of audit log events. To list newest events first, specify `desc`. To list oldest events first, specify `asc`.
The default is `desc`.

Can be one of: `desc`, `asc`

`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 "Get the audit log for an organization"

Status code	Description
`200`	OK

Code samples for "Get the audit log for an organization"

GET /orgs/{org}/audit-log

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" \
http(s)://HOSTNAME/api/v3/orgs/ORG/audit-log
```

Response

Example response Response schema

```
Status: 200
```

```
[ { "actor_ip": "88.123.45.123", "from": "pull_requests#merge", "device_cookie": null, "actor": "mona-admin", "actor_id": 7, "repo": 
"octo-org/octo-repo", "repo_id": 17, "business": "github", "business_id": 1, "org": "octo-org", "org_id": 8, "action": 
"pull_request.merge", "@timestamp": 1635940599755, "created_at": 1635940599755, "operation_type": "modify", "actor_location": { 
"country_code": "GB", "country_name": "United Kingdom", "region": "ENG", "region_name": "England", "city": "Louth", "postal_code": 
"LN11", "location": { "lat": 53.4457, "lon": 0.141 } }, "data": { "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) ...", 
"method": "POST", "request_id": "e4dabc4d-ba16-4bca-1234-649be7ae1188", "server_id": "5d17aab5-fd9f-abcd-a820-16bed246441b", 
```

List app installations for an organization

✓ Works with GitHub Apps

Lists all GitHub Apps in an organization. The installation count includes all GitHub Apps installed on repositories in the organization. You must be an organization owner with `admin:read` scope to use this endpoint.

Parameters for "List app installations 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.

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 app installations for an organization"

Status code	Description
`200`	OK

Code samples for "List app installations for an organization"

GET `/orgs/{org}/installations`

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" \
 curl -L \ -H "Accept: application/vnd.github+json" \ -H "Authorization: Bearer <YOUR-TOKEN>" \ -H "X-GitHub-Api-Version: 2022-11-28" \
http(s)://HOSTNAME/api/v3/orgs/ORG/installations
```

Response

Example response Response schema

Status: 200

```
 { "total_count": 1, "installations": [ { "id": 25381, "account": { "login": "octo-org", "id": 6811672, "node_id":
"MDEyOk9yZ2FuaXphdGlvbjY4MTE2NzI=", "avatar_url": "https://avatars3.githubusercontent.com/u/6811672?v=4", "gravatar_id": "", "url":
"https://HOSTNAME/users/octo-org", "html_url": "https://github.com/octo-org", "followers_url": "https://HOSTNAME/users/octo-
org/followers", "following_url": "https://HOSTNAME/users/octo-org/following{/other_user}", "gists_url": "https://HOSTNAME/users/octo-
org/gists{/gist_id}", "starred_url": "https://HOSTNAME/users/octo-org/starred{/owner}{/repo}", "subscriptions_url":
"https://HOSTNAME/users/octo-org/subscriptions", "organizations_url": "https://HOSTNAME/users/octo-org/orgs", "repos_url":
```

Enable or disable a security feature for an organization

✓ Works with GitHub Apps

Enables or disables the specified security feature for all eligible repositories in an organization.

To use this endpoint, you must be an organization owner or be member of a team with the security manager role. A token with the 'write:org' scope is also required.

GitHub Apps must have the `organization_administration:write` permission to use this endpoint.

For more information, see "Managing security managers in your organization."

Parameters for "Enable or disable a security feature 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.

`security_product` string Required

The security feature to enable or disable.

Can be one of: `dependency_graph`, `dependabot_alerts`, `dependabot_security_updates`, `advanced_security`, `code_scanning_default_setup`, `secret_scanning`, `secret_scanning_push_protection`

`enablement` string Required

The action to take.
`enable_all` means to enable the specified security feature for all repositories in the organization. `disable_all` means to disable the specified security feature for all repositories in the organization.

Can be one of: `enable_all`, `disable_all`

HTTP response status codes for "Enable or disable a security feature for an organization"

Status code	Description
`204`	Action started
`422`	The action could not be taken due to an in progress enablement, or a policy is preventing enablement

Code samples for "Enable or disable a security feature for an organization"

POST /orgs/{org}/{security_product}/{enablement}

cURL JavaScript GitHub CLI

```
curl -L \ -X POST \ -H "Accept: application/vnd.github+json" \ -H "Authorization: Bearer <YOUR-TOKEN>" \ -H "X-GitHub-Api-Version: 2022-11-28" \ http(s)://HOSTNAME/api/v3/orgs/ORG/SECURITY_PRODUCT/ENABLEMENT
```

Action started

```
Status: 204
```

List organizations for the authenticated user

List organizations for the authenticated user.

OAuth scope requirements

This only lists organizations that your authorization allows you to operate on in some way (e.g., you can list teams with `read:org` scope, you can publicize your organization membership with `user` scope, etc.). Therefore, this API requires at least `user` or `read:org` scope. OAuth requests with insufficient scope receive a `403 Forbidden` response.

Parameters for "List organizations for the authenticated user"

Headers

accept string

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

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 organizations for the authenticated user"

Status code	Description
`200`	OK
`304`	Not modified
`401`	Requires authentication
`403`	Forbidden

Code samples for "List organizations for the authenticated user"

GET `/user/orgs`

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" \
http(s)://HOSTNAME/api/v3/user/orgs
```

Response

Example response Response schema

`Status: 200`

```
[ { "login": "github", "id": 1, "node_id": "MDEyOk9yZ2FuaXphdGlvbjE=", "url": "https://HOSTNAME/orgs/github", "repos_url":
"https://HOSTNAME/orgs/github/repos", "events_url": "https://HOSTNAME/orgs/github/events", "hooks_url":
"https://HOSTNAME/orgs/github/hooks", "issues_url": "https://HOSTNAME/orgs/github/issues", "members_url":
"https://HOSTNAME/orgs/github/members{/member}", "public_members_url": "https://HOSTNAME/orgs/github/public_members{/member}",
"avatar_url": "https://github.com/images/error/octocat_happy.gif", "description": "A great organization" } ]
```

List organizations for a user

✓ Works with GitHub Apps

List public organization memberships for the specified user.

This method only lists *public* memberships, regardless of authentication. If you need to fetch all of the organization memberships (public and private) for the authenticated user, use the List organizations for the authenticated user API instead.

Parameters for "List organizations for a user"

Headers

`accept` string

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

Path parameters

`username` string Required

The handle for the GitHub user account.

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 organizations for a user"

Status code	Description
`200`	OK

Code samples for "List organizations for a user"

GET `/users/{username}/orgs`

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" \
http(s)://HOSTNAME/api/v3/users/USERNAME/orgs
```

Response

Example response Response schema

`Status: 200`

```
 [ { "login": "github", "id": 1, "node_id": "MDEyOk9yZ2FuaXphdGlvbjE=", "url": "https://HOSTNAME/orgs/github", "repos_url":
"https://HOSTNAME/orgs/github/repos", "events_url": "https://HOSTNAME/orgs/github/events", "hooks_url":
"https://HOSTNAME/orgs/github/hooks", "issues_url": "https://HOSTNAME/orgs/github/issues", "members_url":
"https://HOSTNAME/orgs/github/members{/member}", "public_members_url": "https://HOSTNAME/orgs/github/public_members{/member}",
"avatar_url": "https://github.com/images/error/octocat_happy.gif", "description": "A great organization" } ]
```

Legal

Terms Privacy Status Pricing Expert services Blog