

REST API / Actions / Secrets

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

# **GitHub Actions Secrets**

Use the REST API to interact with secrets in GitHub Actions.

# **About secrets in GitHub Actions**

You can use the REST API to create, update, delete, and retrieve information about secrets that can be used in workflows in GitHub Actions. Secrets allow you to store sensitive information, such as access tokens, in your repository, repository environments, or organization. For more information, see "<u>Using secrets in GitHub Actions</u>."

# List organization secrets @

Works with <u>GitHub Apps</u>

Lists all secrets available in an organization without revealing their encrypted values.

You must authenticate using an access token with the <code>admin:org</code> scope to use this endpoint. If the repository is private, you must use an access token with the <code>repo</code> scope. GitHub Apps must have the <code>secrets</code> organization permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

# Parameters for "List organization secrets"

### **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 organization secrets"

Status code Description

200 OK

#### Code samples for "List organization secrets"



#### Response

```
Example response Response schema

Status: 200

{ "total_count": 3, "secrets": [ { "name": "GIST_ID", "created_at": "2019-08-10T14:59:22Z", "updated_at": "2020-01-10T14:59:22Z", "visibility": "private" }, { "name": "DEPLOY_TOKEN", "created_at": "2019-08-10T14:59:22Z", "updated_at": "2020-01-10T14:59:22Z", "visibility": "all" }, { "name": "GH_TOKEN", "created_at": "2019-08-10T14:59:22Z", "updated_at": "2020-01-10T14:59:22Z", "visibility": "selected", "selected_repositories_url": "https://HOSTNAME/orgs/octo-org/actions/secrets/SUPER_SECRET/repositories" } ]
}
```

# Get an organization public key &

### Works with <u>GitHub Apps</u>

Gets your public key, which you need to encrypt secrets. You need to encrypt a secret before you can create or update secrets.

You must authenticate using an access token with the <code>admin:org</code> scope to use this endpoint. If the repository is private, you must use an access token with the <code>repo</code> scope. GitHub Apps must have the <code>secrets</code> organization permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

# Parameters for "Get an organization public key"

#### 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 public key"

Status code	Description
200	OK

#### Code samples for "Get an organization public key"



#### Response

```
Example response Response schema

Status: 200

{ "key_id": "012345678912345678", "key": "2Sg8iYjAxxmI2LvUXpJjkYrMxURPc8r+dB7TJyvv1234" }
```

# Get an organization secret &

Works with <u>GitHub Apps</u>

Gets a single organization secret without revealing its encrypted value.

You must authenticate using an access token with the <code>admin:org</code> scope to use this endpoint. If the repository is private, you must use an access token with the <code>repo</code> scope. GitHub Apps must have the <code>secrets</code> organization permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

# Parameters for "Get an organization secret"

# 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.

secret\_name string Required

HTTP response status codes for "Get an organization secret"

Status code Description

200 OK

#### Code samples for "Get an organization secret"



#### Response

The name of the secret.

Example response Response schema

Status: 200

{ "name": "GH\_TOKEN", "created\_at": "2019-08-10T14:59:22Z", "updated\_at": "2020-01-10T14:59:22Z", "visibility": "selected", "selected\_repositories\_url": "https://HOSTNAME/orgs/octo-org/actions/secrets/SUPER\_SECRET/repositories" }

# Create or update an organization secret $\mathscr O$

# Works with <u>GitHub Apps</u>

Creates or updates an organization secret with an encrypted value. Encrypt your secret using <u>LibSodium</u>. For more information, see "<u>Encrypting secrets for the REST API</u>."

You must authenticate using an access token with the <code>admin:org</code> scope to use this endpoint. If the repository is private, you must use an access token with the <code>repo</code> scope. GitHub Apps must have the <code>secrets</code> organization permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

# Parameters for "Create or update an organization secret"

#### 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.

secret\_name string Required

The name of the secret.

#### **Body parameters**

#### encrypted\_value string

Value for your secret, encrypted with LibSodium using the public key retrieved from the Get an organization public key endpoint.

key\_id string

ID of the key you used to encrypt the secret.

#### visibility string Required

Which type of organization repositories have access to the organization secret. selected means only the repositories specified by selected\_repository\_ids can access the secret.

Can be one of: all, private, selected

#### selected\_repository\_ids array of integers

An array of repository ids that can access the organization secret. You can only provide a list of repository ids when the visibility is set to selected. You can manage the list of selected repositories using the <u>List selected repositories for an organization secret</u>, <u>Set selected repositories for an organization secret</u>, and <u>Remove selected repository from an organization secret</u> endpoints.

# HTTP response status codes for "Create or update an organization secret"

Status code	Description
201	Response when creating a secret
204	Response when updating a secret

# Code samples for "Create or update an organization secret"

Example 1: Status Code 201 (application/json) \$

PUT /orgs/{org}/actions/secrets/{secret\_name}

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" \ http(s)://HOSTNAME/api/v3/orgs/ORG/actions/secrets/SECRET\_NAME \ -d

ф

'{"encrypted\_value":"c2VjcmV0","key\_id":"012345678912345678","visibility":"selected","selected\_repository\_ids":[1296269,1296280]}'

Example response Response schema
Status: 201

# Delete an organization secret &

Works with <u>GitHub Apps</u>

Deletes a secret in an organization using the secret name.

You must authenticate using an access token with the <code>admin:org</code> scope to use this endpoint. If the repository is private, you must use an access token with the <code>repo</code> scope. GitHub Apps must have the <code>secrets</code> organization permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

# Parameters for "Delete an organization secret"

#### **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.

secret\_name string Required

The name of the secret.

# HTTP response status codes for "Delete an organization secret"

Status code	Description
204	No Content

# Code samples for "Delete an organization secret"



# List selected repositories for an organization secret &

# Works with <u>GitHub Apps</u>

Lists all repositories that have been selected when the visibility for repository access to a secret is set to selected.

You must authenticate using an access token with the <code>admin:org</code> scope to use this endpoint. If the repository is private, you must use an access token with the <code>repo</code> scope. GitHub Apps must have the <code>secrets</code> organization permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

#### Parameters for "List selected repositories for an organization secret"

#### **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.

secret\_name string Required

The name of the secret.

#### **Query parameters**

page integer

Page number of the results to fetch.

Default: 1

per\_page integer

The number of results per page (max 100).

Default: 30

# HTTP response status codes for "List selected repositories for an organization secret"

Status code Description

200 OK

# Code samples for "List selected repositories for an organization secret"

GET /orgs/{org}/actions/secrets/{secret\_name}/repositories

```
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/actions/secrets/SECRET_NAME/repositories
```

#### 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://HOSTNAME/users/octocat", "html_url": "https://github.com/octocat", "followers_url": "https://HOSTNAME/users/octocat/following_url": "https://HOSTNAME/users/octocat/following_url": "https://HOSTNAME/users/octocat/gists{/gist_id}", "starred_url": "https://HOSTNAME/users/octocat/starred{/owner}{/repo}", "subscriptions_url": "*
```

# Set selected repositories for an organization secret @

# Works with <u>GitHub Apps</u>

Replaces all repositories for an organization secret when the visibility for repository access is set to selected. The visibility is set when you <u>Create or update an organization secret</u>.

You must authenticate using an access token with the <code>admin:org</code> scope to use this endpoint. If the repository is private, you must use an access token with the <code>repo</code> scope. GitHub Apps must have the <code>secrets</code> organization permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

#### Parameters for "Set selected repositories for an organization secret"

#### **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.

secret\_name string Required

The name of the secret.

#### **Body parameters**

selected\_repository\_ids array of integers Required

An array of repository ids that can access the organization secret. You can only provide a list of repository ids when the visibility is set to selected. You can add and remove individual repositories using the Add selected repository to an organization secret and

# HTTP response status codes for "Set selected repositories for an organization secret"

Status code Description

204 No Content

#### Code samples for "Set selected repositories for an organization secret"

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" \ http(s)://HOSTNAME/api/v3/orgs/ORG/actions/secrets/SECRET\_NAME/repositories \ -d '{"selected\_repository\_ids": [64780797]}'

#### Response

Status: 204

# Add selected repository to an organization secret &

Works with <u>GitHub Apps</u>

Adds a repository to an organization secret when the visibility for repository access is set to selected. The visibility is set when you <u>Create or update an organization secret</u>.

You must authenticate using an access token with the <code>admin:org</code> scope to use this endpoint. If the repository is private, you must use an access token with the <code>repo</code> scope. GitHub Apps must have the <code>secrets</code> organization permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

# Parameters for "Add selected repository to an organization secret"

### 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.

secret\_name string Required

The name of the secret

The hame of the secreti

repository\_id integer Required

# HTTP response status codes for "Add selected repository to an organization secret"

Status code	Description
204	No Content when repository was added to the selected list
409	Conflict when visibility type is not set to selected

### Code samples for "Add selected repository to an organization secret"



#### No Content when repository was added to the selected list

Status: 204

# Remove selected repository from an organization secret @

Works with <u>GitHub Apps</u>

Removes a repository from an organization secret when the visibility for repository access is set to selected. The visibility is set when you <u>Create or update an organization secret</u>.

You must authenticate using an access token with the <code>admin:org</code> scope to use this endpoint. If the repository is private, you must use an access token with the <code>repo</code> scope. GitHub Apps must have the <code>secrets</code> organization permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

# Parameters for "Remove selected repository from an organization secret"

# 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.

secret\_name string Required

repository\_id integer Required

The name of the secret.

# HTTP response status codes for "Remove selected repository from an organization secret"

Status code	Description
204	Response when repository was removed from the selected list
409	Conflict when visibility type not set to selected

# Code samples for "Remove selected repository from an organization secret"



#### Response when repository was removed from the selected list

Status: 204

# List repository organization secrets &

Works with GitHub Apps

Lists all organization secrets shared with a repository without revealing their encrypted values.

You must authenticate using an access token with the repo scope to use this endpoint. GitHub Apps must have the secrets repository permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

#### Parameters for "List repository organization secrets"

#### **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.

#### **Query parameters**

per\_page integer

The number of results per page (max 100).

Default: 30

page integer

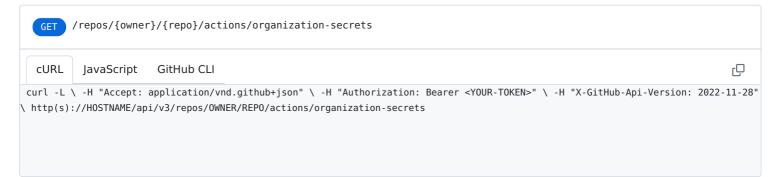
Page number of the results to fetch.

Default: 1

# HTTP response status codes for "List repository organization secrets"

Status code	Description
200	ОК

# Code samples for "List repository organization secrets"



# Response

```
Example response Response schema

Status: 200

{ "total_count": 2, "secrets": [ { "name": "GH_TOKEN", "created_at": "2019-08-10T14:59:22Z", "updated_at": "2020-01-10T14:59:22Z" }, 
{ "name": "GIST_ID", "created_at": "2020-01-10T10:59:22Z", "updated_at": "2020-01-11T11:59:22Z" } ]
```

# **List repository secrets** *∂*

Works with <u>GitHub Apps</u>

Lists all secrets available in a repository without revealing their encrypted values.

You must authenticate using an access token with the repo scope to use this endpoint. GitHub Apps must have the secrets repository permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

# Parameters for "List repository secrets"

#### **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.

#### **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 repository secrets"

Status code	Description
200	OK

# Code samples for "List repository secrets"



#### Response

Example response Response schema
Status: 200

```
{ "total_count": 2, "secrets": [ { "name": "GH_TOKEN", "created_at": "2019-08-10T14:59:22Z", "updated_at": "2020-01-10T14:59:22Z" }, { "name": "GIST_ID", "created_at": "2020-01-10T10:59:22Z", "updated_at": "2020-01-11T11:59:22Z" } ] }
```

# Get a repository public key ∂

Works with GitHub Apps

Gets your public key, which you need to encrypt secrets. You need to encrypt a secret before you can create or update secrets.

Anyone with read access to the repository can use this endpoint. If the repository is private you must use an access token with the repo scope. GitHub Apps must have the secrets repository permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

# Parameters for "Get a repository public key"

#### **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 a repository public key"

Status code	Description
200	ОК

# Code samples for "Get a repository public key"



#### Response

```
Example response Response schema

Status: 200

{ "key_id": "012345678912345678", "key": "2Sg8iYjAxxmI2LvUXpJjkYrMxURPc8r+dB7TJyvv1234" }
```

# Get a repository secret ∂

Works with <u>GitHub Apps</u>

Gets a single repository secret without revealing its encrypted value.

You must authenticate using an access token with the repo scope to use this endpoint. GitHub Apps must have the secrets repository permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

# Parameters for "Get a repository secret"

#### **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.

secret\_name string Required

The name of the secret.

# HTTP response status codes for "Get a repository secret"

Status code	Description
200	OK

# Code samples for "Get a repository secret"

GET /repos/{owner}/{repo}/actions/secrets/{secret\_name}

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/repos/OWNER/REPO/actions/secrets/SECRET\_NAME

### Response

```
Example response Response schema

Status: 200

{ "name": "GH_TOKEN", "created_at": "2019-08-10T14:59:22Z", "updated_at": "2020-01-10T14:59:22Z" }
```

# Create or update a repository secret ∂

Works with GitHub Apps

Creates or updates a repository secret with an encrypted value. Encrypt your secret using <u>LibSodium</u>. For more information, see "<u>Encrypting secrets for the REST API</u>."

You must authenticate using an access token with the repo scope to use this endpoint. GitHub Apps must have the secrets repository permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

# Parameters for "Create or update a repository secret"

### **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.

secret\_name string Required

The name of the secret.

### **Body parameters**

encrypted\_value string

Value for your secret, encrypted with LibSodium using the public key retrieved from the Get a repository public key endpoint.

key\_id string

ID of the key you used to encrypt the secret.

# HTTP response status codes for "Create or update a repository secret"

Status code	Description
201	Response when creating a secret
204	Response when updating a secret

# Code samples for "Create or update a repository secret"

Example 1: Status Code 201 (application/json) ♦



### Response when creating a secret

Example response Response schema
Status: 201

# **Delete a repository secret** *∂*

Works with <u>GitHub Apps</u>

Deletes a secret in a repository using the secret name.

You must authenticate using an access token with the repo scope to use this endpoint. GitHub Apps must have the secrets repository permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

# Parameters for "Delete a repository secret"

#### **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.

secret\_name string Required

The name of the secret.

# HTTP response status codes for "Delete a repository secret"

Status code Description

No Content

# Code samples for "Delete a repository secret"

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/repos/OWNER/REPO/actions/secrets/SECRET\_NAME

# Response

Status: 204

# List environment secrets &

Works with <u>GitHub Apps</u>

Lists all secrets available in an environment without revealing their encrypted values.

You must authenticate using an access token with the repo scope to use this endpoint. GitHub Apps must have the secrets repository permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

#### Parameters for "List environment secrets"

#### **Headers**

accept string

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

#### Path parameters

repository\_id integer Required

The unique identifier of the repository.

environment\_name string Required

The name of the environment.

# **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 environment secrets"

Status code	Description
200	ОК

# Code samples for "List environment secrets"



# Response

```
Example response Response schema

Status: 200

{ "total_count": 2, "secrets": [ { "name": "GH_TOKEN", "created_at": "2019-08-10T14:59:22Z", "updated_at": "2020-01-10T14:59:22Z" }, { "name": "GIST_ID", "created_at": "2020-01-10T10:59:22Z", "updated_at": "2020-01-11T11:59:22Z" } ] }
```

# Get an environment public key &

# Works with <u>GitHub Apps</u>

Get the public key for an environment, which you need to encrypt environment secrets. You need to encrypt a secret before you can create or update secrets.

Anyone with read access to the repository can use this endpoint. If the repository is private you must use an access token with the repo scope. GitHub Apps must have the secrets repository permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

#### Parameters for "Get an environment public key"

#### Headers

accept string

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

#### Path parameters

repository\_id integer Required

The unique identifier of the repository.

environment name string Required

The name of the environment.

# HTTP response status codes for "Get an environment public key"

Status code Description

200 OK

# Code samples for "Get an environment public key"

/repositories/{repository\_id}/environments/{environment\_name}/secrets/public-key

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"

ſŪ

\ http(s)://HOSTNAME/api/v3/repositories/REPOSITORY\_ID/environments/ENVIRONMENT\_NAME/secrets/public-key

#### Response

GET

Example response Response schema

Status: 200

{ "key\_id": "012345678912345678", "key": "2Sg8iYjAxxmI2LvUXpJjkYrMxURPc8r+dB7TJyvv1234" }

# Get an environment secret &

Works with GitHub Apps

Gets a single environment secret without revealing its encrypted value.

You must authenticate using an access token with the repo scope to use this endpoint. GitHub Apps must have the secrets repository permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

#### Parameters for "Get an environment secret"

#### **Headers**

accept string

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

#### **Path parameters**

repository\_id integer Required

The unique identifier of the repository.

environment\_name string Required

The name of the environment.

secret\_name string Required

The name of the secret.

# HTTP response status codes for "Get an environment secret"

Status code	Description
200	OK

#### Code samples for "Get an environment secret"



#### Response

```
Example response Response schema

Status: 200

{ "name": "GH_TOKEN", "created_at": "2019-08-10T14:59:22Z", "updated_at": "2020-01-10T14:59:22Z" }
```

# Create or update an environment secret &

Works with <u>GitHub Apps</u>

Creates or updates an environment secret with an encrypted value. Encrypt your secret using <u>LibSodium</u>. For more information, see "<u>Encrypting secrets for the REST API</u>."

You must authenticate using an access token with the repo scope to use this endpoint. GitHub Apps must have the secrets repository permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

#### Parameters for "Create or update an environment secret"

#### Headers

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

#### Path parameters

repository\_id integer Required

The unique identifier of the repository.

environment\_name string Required

The name of the environment.

secret\_name string Required

The name of the secret.

### **Body parameters**

encrypted\_value string Required

Value for your secret, encrypted with LibSodium using the public key retrieved from the Get an environment public key endpoint.

ID of the key you used to encrypt the secret.

# HTTP response status codes for "Create or update an environment secret"

Status code	Description
201	Response when creating a secret
204	Response when updating a secret

### Code samples for "Create or update an environment secret"

Example 1: Status Code 201 (application/json) \$



#### Response when creating a secret

Example response Response schema
Status: 201

# Delete an environment secret @

Works with <u>GitHub Apps</u>

Deletes a secret in an environment using the secret name.

You must authenticate using an access token with the repo scope to use this endpoint. GitHub Apps must have the secrets repository permission to use this endpoint. Authenticated users must have collaborator access to a repository to create, update, or read secrets.

# Parameters for "Delete an environment secret"

# Headers

accept string

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

### **Path parameters**

repository\_id integer Required

The unique identifier of the repository. environment\_name string Required The name of the environment. secret\_name string Required The name of the secret. HTTP response status codes for "Delete an environment secret" Status code **Description** 204 Default response Code samples for "Delete an environment secret" DELETE /repositories/{repository\_id}/environments/{environment\_name}/secrets/{secret\_name} cURL JavaScript GitHub CLI Q 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/repositories/REPOSITORY\_ID/environments/ENVIRONMENT\_NAME/secrets/SECRET\_NAME **Default 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>