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

Secret scanning

Use the REST API to retrieve and update secret alerts from a repository.

Note: The endpoints to manage secret scanning are currently in beta and subject to change.

About secret scanning

You can use the API to:

- Enable or disable secret scanning and push protection for a repository. For more information, see "Repositories" and expand the "Properties of the `security_and_analysis` object" section in the REST API documentation.
- Retrieve and update secret scanning alerts from a repository. For further details, see the sections below.

For more information about secret scanning, see "About secret scanning."

List secret scanning alerts for an enterprise

Lists secret scanning alerts for eligible repositories in an enterprise, from newest to oldest. To use this endpoint, you must be a member of the enterprise, and you must use an access token with the `repo` scope or `security_events` scope. Alerts are only returned for organizations in the enterprise for which you are an organization owner or a security manager.

Parameters for "List secret scanning alerts 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.

Query parameters

`state` string

Set to `open` or `resolved` to only list secret scanning alerts in a specific state.

Can be one of: `open`, `resolved`

`secret_type` string

A comma-separated list of secret types to return. By default all secret types are returned. See "Secret scanning patterns" for a complete list of secret types.

`resolution` string

A comma-separated list of resolutions. Only secret scanning alerts with one of these resolutions are listed. Valid resolutions are `false_positive`, `wont_fix`, `revoked`, `pattern_edited`, `pattern_deleted` or `used_in_tests`.

`sort` string

The property to sort the results by. `created` means when the alert was created. `updated` means when the alert was updated or resolved.

Default: `created`
Can be one of: `created`, `updated`

`direction` string

The direction to sort the results by.

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

`per_page` integer

The number of results per page (max 100).

Default: `30`

`before` string

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

`after` string

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

HTTP response status codes for "List secret scanning alerts for an enterprise"

Status code	Description
`200`	OK
`404`	Resource not found
`503`	Service unavailable

Code samples for "List secret scanning alerts for an enterprise"

GET /enterprises/{enterprise}/secret-scanning/alerts

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/enterprises/ENTERPRISE/secret-scanning/alerts
```

Response

Example response Response schema

```
Status: 200
```

```
[ { "number": 2, "created_at": "2020-11-06T18:48:51Z", "url": "https://HOSTNAME/repos/owner/private-repo/secret-
scanning/alerts/2", "html_url": "https://github.com/owner/private-repo/security/secret-scanning/2", "locations_url":
"https://HOSTNAME/repos/owner/private-repo/secret-scanning/alerts/2/locations", "state": "resolved", "resolution":
"false_positive", "resolved_at": "2020-11-07T02:47:13Z", "resolved_by": { "login": "monalisa", "id": 2, "node_id": "MDQ6VXNlcjI=",
"avatar_url": "https://alambic.github.com/avatars/u/2?", "gravatar_id": "", "url": "https://HOSTNAME/users/monalisa", "html_url":
"https://github.com/monalisa", "followers_url": "https://HOSTNAME/users/monalisa/followers", "following_url":
```

List secret scanning alerts for an organization

Works with GitHub Apps

Lists secret scanning alerts for eligible repositories in an organization, from newest to oldest. To use this endpoint, you must be an administrator or security manager for the organization, and you must use an access token with the `repo` scope or `security_events` scope. For public repositories, you may instead use the `public_repo` scope.

GitHub Apps must have the `secret_scanning_alerts` read permission to use this endpoint.

Parameters for "List secret scanning alerts 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

`state` string

Set to `open` or `resolved` to only list secret scanning alerts in a specific state.

Can be one of: `open`, `resolved`

`secret_type` string

A comma-separated list of secret types to return. By default all secret types are returned. See "Secret scanning patterns" for a complete list of secret types.

`resolution` string

A comma-separated list of resolutions. Only secret scanning alerts with one of these resolutions are listed. Valid resolutions are `false_positive`, `wont_fix`, `revoked`, `pattern_edited`, `pattern_deleted` or `used_in_tests`.

`sort` string

The property to sort the results by. `created` means when the alert was created. `updated` means when the alert was updated or resolved.

Default: `created`
Can be one of: `created`, `updated`

`direction` string

The direction to sort the results by.

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

`page` integer

Page number of the results to fetch.

Default: `1`

`per_page` integer

The number of results per page (max 100).

Default: `30`

`before` string

A cursor, as given in the Link header. If specified, the query only searches for events before this cursor. To receive an initial cursor on your first request, include an empty "before" query string.

`after` string

A cursor, as given in the Link header. If specified, the query only searches for events after this cursor. To receive an initial cursor on your first request, include an empty "after" query string.

HTTP response status codes for "List secret scanning alerts for an organization"

Status code	Description
`200`	OK
`404`	Resource not found
`503`	Service unavailable

Code samples for "List secret scanning alerts for an organization"

GET /orgs/{org}/secret-scanning/alerts

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/secret-scanning/alerts
```

Response

Example response Response schema

Status: 200

[{ "number": 2, "created_at": "2020-11-06T18:48:51Z", "url": "https://HOSTNAME/repos/owner/private-repo/secret-scanning/alerts/2", "html_url": "https://github.com/owner/private-repo/security/secret-scanning/2", "locations_url": "https://HOSTNAME/repos/owner/private-repo/secret-scanning/alerts/2/locations", "state": "resolved", "resolution": "false_positive", "resolved_at": "2020-11-07T02:47:13Z", "resolved_by": { "login": "monalisa", "id": 2, "node_id": "MDQ6VXNlcjI=", "avatar_url": "https://alambic.github.com/avatars/u/2?", "gravatar_id": "", "url": "https://HOSTNAME/users/monalisa", "html_url": "https://github.com/monalisa", "followers_url": "https://HOSTNAME/users/monalisa/followers", "following_url":

List secret scanning alerts for a repository

✓ Works with [GitHub Apps](#)

Lists secret scanning alerts for an eligible repository, from newest to oldest. To use this endpoint, you must be an administrator for the repository or for the organization that owns the repository, and you must use a personal access token with the `repo` scope or `security_events` scope. For public repositories, you may instead use the `public_repo` scope.

GitHub Apps must have the `secret_scanning_alerts` read permission to use this endpoint.

Parameters for "List secret scanning alerts 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.

Query parameters

`state` string

Set to `open` or `resolved` to only list secret scanning alerts in a specific state.

Can be one of: `open`, `resolved`

`secret_type` string

A comma-separated list of secret types to return. By default all secret types are returned. See "[Secret scanning patterns](#)" for a complete list of secret types.

`resolution` string

A comma-separated list of resolutions. Only secret scanning alerts with one of these resolutions are listed. Valid resolutions are `false_positive`, `wont_fix`, `revoked`, `pattern_edited`, `pattern_deleted` or `used_in_tests`.

`sort` string

The property to sort the results by. `created` means when the alert was created. `updated` means when the alert was updated or resolved.

Default: `created`
Can be one of: `created`, `updated`

`direction` string

The direction to sort the results by.

Default: `desc`

Default: desc

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

`page` integer

Page number of the results to fetch.

Default: `1`

`per_page` integer

The number of results per page (max 100).

Default: `30`

`before` string

A cursor, as given in the Link header. If specified, the query only searches for events before this cursor. To receive an initial cursor on your first request, include an empty "before" query string.

`after` string

A cursor, as given in the Link header. If specified, the query only searches for events after this cursor. To receive an initial cursor on your first request, include an empty "after" query string.

HTTP response status codes for "List secret scanning alerts for a repository"

Status code	Description
`200`	OK
`404`	Repository is public or secret scanning is disabled for the repository
`503`	Service unavailable

Code samples for "List secret scanning alerts for a repository"

GET /repos/{owner}/{repo}/secret-scanning/alerts

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/secret-scanning/alerts
```

Response

Example response Response schema

Status: 200

```
[ { "number": 2, "created_at": "2020-11-06T18:48:51Z", "url": "https://HOSTNAME/repos/owner/private-repo/secret-scanning/alerts/2", "html_url": "https://github.com/owner/private-repo/security/secret-scanning/2", "locations_url": "https://HOSTNAME/repos/owner/private-repo/secret-scanning/alerts/2/locations", "state": "resolved", "resolution": "false_positive", "resolved_at": "2020-11-07T02:47:13Z", "resolved_by": { "login": "monalisa", "id": 2, "node_id": "MDQ6VXNlcjI=", "avatar_url": "https://alambic.github.com/avatars/u/2?", "gravatar_id": "", "url": "https://HOSTNAME/users/monalisa", "html_url":
```

"https://github.com/monalisa", "followers_url": "https://HOSTNAME/users/monalisa/followers", "following_url":

Get a secret scanning alert

✓ Works with GitHub Apps

Gets a single secret scanning alert detected in an eligible repository. To use this endpoint, you must be an administrator for the repository or for the organization that owns the repository, and you must use a personal access token with the `repo` scope or `security_events` scope. For public repositories, you may instead use the `public_repo` scope.

GitHub Apps must have the `secret_scanning_alerts` read permission to use this endpoint.

Parameters for "Get a secret scanning alert"

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.

`alert_number` integer Required

The number that identifies an alert. You can find this at the end of the URL for a code scanning alert within GitHub, and in the `number` field in the response from the `GET /repos/{owner}/{repo}/code-scanning/alerts` operation.

HTTP response status codes for "Get a secret scanning alert"

Status code	Description
`200`	OK
`304`	Not modified
`404`	Repository is public, or secret scanning is disabled for the repository, or the resource is not found
`503`	Service unavailable

Code samples for "Get a secret scanning alert"

GET /repos/{owner}/{repo}/secret-scanning/alerts/{alert_number}

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/secret-scanning/alerts/ALERT_NUMBER
```

Response

Example response   Response schema

```
Status: 200
```

```
{ "number": 42, "created_at": "2020-11-06T18:18:30Z", "url": "https://HOSTNAME/repos/owner/private-repo/secret-scanning/alerts/42",
"html_url": "https://github.com/owner/private-repo/security/secret-scanning/42", "locations_url":
"https://HOSTNAME/repos/owner/private-repo/secret-scanning/alerts/42/locations", "state": "open", "secret_type": "mailchimp_api_key",
"secret_type_display_name": "Mailchimp API Key", "secret": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX-us2", "push_protection_bypassed": false
}
```

Update a secret scanning alert

✓ Works with GitHub Apps

Updates the status of a secret scanning alert in an eligible repository. To use this endpoint, you must be an administrator for the repository or for the organization that owns the repository, and you must use a personal access token with the `repo` scope or `security_events` scope. For public repositories, you may instead use the `public_repo` scope.

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

Parameters for "Update a secret scanning alert"

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.

`alert_number` integer Required

The number that identifies an alert. You can find this at the end of the URL for a code scanning alert within GitHub, and in the `number` field in the response from the `GET /repos/{owner}/{repo}/code-scanning/alerts` operation.

Body parameters

`state` string Required

Sets the state of the secret scanning alert. You must provide `resolution` when you set the state to `resolved`.

Can be one of: `open`, `resolved`

`resolution` string or null

Required when the `state` is `resolved`. The reason for resolving the alert.

Can be one of: `false_positive`, `wont_fix`, `revoked`, `used_in_tests`, *`null`*

`resolution_comment` string or null

An optional comment when closing an alert. Cannot be updated or deleted. Must be `null` when changing `state` to `open`.

HTTP response status codes for "Update a secret scanning alert"

Status code	Description
`200`	OK
`400`	Bad request, resolution comment is invalid or the resolution was not changed.
`404`	Repository is public, or secret scanning is disabled for the repository, or the resource is not found
`422`	State does not match the resolution or resolution comment
`503`	Service unavailable

Code samples for "Update a secret scanning alert"

PATCH /repos/{owner}/{repo}/secret-scanning/alerts/{alert_number}

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/repos/OWNER/REPO/secret-scanning/alerts/ALERT_NUMBER \ -d '{"state":"resolved","resolution":"false_positive"}'
```

Response

Example response Response schema

```
Status: 200
```

```
{ "number": 42, "created_at": "2020-11-06T18:18:30Z", "url": "https://HOSTNAME/repos/owner/private-repo/secret-scanning/alerts/42", "html_url": "https://github.com/owner/private-repo/security/secret-scanning/42", "locations_url": "https://HOSTNAME/repos/owner/private-repo/secret-scanning/alerts/42/locations", "state": "resolved", "resolution": "used_in_tests", "resolved_at": "2020-11-16T22:42:07Z", "resolved_by": { "login": "monalisa", "id": 2, "node_id": "MDQ6VXNlcjI=", "avatar_url": "https://alambic.github.com/avatars/u/2?", "gravatar_id": "", "url": "https://HOSTNAME/users/monalisa", "html_url": "https://github.com/monalisa", "followers_url": "https://HOSTNAME/users/monalisa/followers", "following_url":
```

List locations for a secret scanning alert

Works with GitHub Apps

Lists all locations for a given secret scanning alert for an eligible repository. To use this endpoint, you must be an administrator for the repository or for the organization that owns the repository, and you must use a personal access token with the `repo` scope or `security_events` scope. For public repositories, you may instead use the `public_repo` scope.

GitHub Apps must have the `secret_scanning_alerts` read permission to use this endpoint.

Parameters for "List locations for a secret scanning alert"

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.

`alert_number` integer Required

The number that identifies an alert. You can find this at the end of the URL for a code scanning alert within GitHub, and in the `number` field in the response from the `GET /repos/{owner}/{repo}/code-scanning/alerts` operation.

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 locations for a secret scanning alert"

Status code	Description
`200`	OK
`404`	Repository is public, or secret scanning is disabled for the repository, or the resource is not found
`503`	Service unavailable

Code samples for "List locations for a secret scanning alert"

GET /repos/{owner}/{repo}/secret-scanning/alerts/{alert_number}/locations

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/secret-scanning/alerts/ALERT_NUMBER/locations
```

Response

Example response   Response schema

```
Status: 200
```

```
[ { "type": "commit", "details": { "path": "/example/secrets.txt", "start_line": 1, "end_line": 1, "start_column": 1,
"end_column": 64, "blob_sha": "af5626b4a114abcb82d63db7c8082c3c4756e51b", "blob_url": "https://HOSTNAME/repos/octocat/hello-
world/git/blobs/af5626b4a114abcb82d63db7c8082c3c4756e51b", "commit_sha": "f14d7debf9775f957cf4f1e8176da0786431f72b", "commit_url":
"https://HOSTNAME/repos/octocat/hello-world/git/commits/f14d7debf9775f957cf4f1e8176da0786431f72b" } }, { "type": "issue_title",
"details": { "issue_title_url": "https://HOSTNAME/repos/octocat/Hello-World/issues/1347" } }, { "type": "issue_body", "details": {
"issue_body_url": "https://HOSTNAME/repos/octocat/Hello-World/issues/1347" } }, { "type": "issue_comment", "details": {
```

Legal

Terms Privacy Status Pricing Expert services Blog