

The REST API is now versioned. For more information, see ["About API versioning."](#)

Code security and analysis

Use the REST API to manage code security and analysis features for your enterprise.

These endpoints only support authentication using a personal access token (classic). For more information, see ["Managing your personal access tokens."](#)

Get code security and analysis features for an enterprise

Gets code security and analysis settings for the specified enterprise. To use this endpoint, you must be an administrator of the enterprise, and you must use an access token with the `admin:enterprise` scope.

Parameters for "Get code security and analysis features 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 code security and analysis features for an enterprise"

Status code	Description
200	OK
404	Resource not found

Code samples for "Get code security and analysis features for an enterprise"


GET

/enterprises/{enterprise}/code_security_and_analysis

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/code_security_and_analysis
```

Response

Example response

Response schema

Status: 200

```
{ "advanced_security_enabled_for_new_repositories": true, "dependabot_alerts_enabled_for_new_repositories": true, "secret_scanning_enabled_for_new_repositories": true, "secret_scanning_push_protection_enabled_for_new_repositories": true, "secret_scanning_push_protection_custom_link": "https://github.com/test-org/test-repo/blob/main/README.md" }
```

Update code security and analysis features for an enterprise

Updates the settings for advanced security, Dependabot alerts, secret scanning, and push protection for new repositories in an enterprise. To use this endpoint, you must be an administrator of the enterprise, and you must use an access token with the `admin:enterprise` scope.

Parameters for "Update code security and analysis features 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

`advanced_security_enabled_for_new_repositories` `boolean`

Whether GitHub Advanced Security is automatically enabled for new repositories. For more information, see "[About GitHub Advanced Security](#)."

`dependabot_alerts_enabled_for_new_repositories` `boolean`

Whether Dependabot alerts are automatically enabled for new repositories. For more information, see "[About Dependabot alerts](#)."

`secret_scanning_enabled_for_new_repositories` `boolean`

Whether secret scanning is automatically enabled for new repositories. For more information, see "[About secret scanning](#)."

`secret_scanning_push_protection_enabled_for_new_repositories` `boolean`

Whether secret scanning push protection is automatically enabled for new repositories. For more information, see "[Protecting pushes with secret scanning](#)."

`secret_scanning_push_protection_custom_link` `string or null`

The URL that will be displayed to contributors who are blocked from pushing a secret. For more information, see "[Protecting pushes with secret scanning](#)." To disable this functionality, set this field to `null`.

HTTP response status codes for "Update code security and analysis features for an enterprise"

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

Code samples for "Update code security and analysis features for an enterprise"

PATCH

/enterprises/{enterprise}/code_security_and_analysis

cURL

JavaScriptGitHub 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/enterprises/ENTERPRISE/c
ode_security_and_analysis \
-p '{"advanced_security_enabled_for_new_repositories":true,"advanced_security_enabled_new_user_namespace_repos":true,"dependabot_alerts_enabled_for_new_repositories":true,"secret_scanning_enabled_for_new_repositories":true,"secret_scanning_push_protection_enabled_for_new_repositories":true,"secret_scanning_push_protection_custom_link":null}'
```

Action started

Status: 204

Enable or disable a security feature

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

To use this endpoint, you must be an administrator of the enterprise, and you must use an access token with the `admin:enterprise` scope.

Parameters for "Enable or disable a security feature"

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.

`security_product` `string` **Required**

The security feature to enable or disable.

Can be one of: `advanced_security`, `dependabot_alerts`, `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 enterprise. `disable_all` means to disable the specified security feature for all repositories in the enterprise.

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

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

Status code	Description
204	Action started

Code samples for "Enable or disable a security feature"

POST

/enterprises/{enterprise}/{security_product}/{enablement}

cURL

JavaScriptGitHub 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/enterprises/ENTERPRISE/SECURITY_PRODUCT/ENABLEMENT

Action started

Status: 204

Legal