Logpresso Sonar REST API Reference

## Query API

### Query

Runs a Logpresso query, waits for it to complete, and then retrieves the query results. For queries that take a long time, it is recommended to use the [Create Cursor](https://docs.logpresso.com/en/sonar/4.0/api/create-cursor) API as timeouts may occur depending on client settings. If you disconnect the HTTP connection, the query you were executing is immediately canceled.

#### HTTP Request

GET /api/sonar/query

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ "https://HOSTNAME/api/sonar/query?q=system+tables"

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| q | O | String | Logpresso query string |  |
| offset | X | 64-bit integer | Number of records to skip | Minimum 0. Default 0 |
| limit | X | 64-bit integer | Maximum number of records to load | Minimum 0. If not specified, load all records |
| fields | X | String | List of output field names | Comma-separated list |
| format | X | String | Output format | One of the following: html, xml, csv, json. |

#### Success Response

Below is an example response to a system tables | fields table query. If text/html is given in the Accept header, it will be output in HTML format. Otherwise, it will be output in newline-delimited JSON format.

{"table":"sonar\_event\_00001"}{"table":"sonar\_raw\_event\_00001"}

#### Error Responses

Missing query argument

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "q should be not null"}

Invalid query

HTTP status code 400

{ "error\_code": "invalid-query", "error\_msg": "(10200) missing-json-quotation"}

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "offset should be long type."}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "offset should be non-negative integer."}

Invalid format value

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "format should be html, xml, csv, or json."}

### Get Query Status

Gets the status of a specific foreground or background query executed by the user in the current session.

#### HTTP Request

GET /api/sonar/queries/:id

#### Success Response

{ "id": 60, "source": "adhoc", "login\_name": "xeraph", "remote\_ip": "0:0:0:0:0:0:0:1", "rows": 32, "elapsed": 21, "is\_finished": true, "is\_cancelled": false, "is\_scheduled\_query": false, "constants": {}, "query\_string": "system tables", "start\_time": 1663044689188, "finish\_time": 1663044689209, "last\_started": "2022-09-13 13:51:29+0900", "background": false, "commands": [ { "command": "system tables", "status": "End" "push\_count": 32, } ], "sub\_queries": [], "stamp": 5, "tags": {}}

* **id** (32-bit integer): Query ID
* **source** (String): Query execution type
* User input (adhoc)
* Logpresso shell (console)
* Scheduled query (scheduled-query)
* REST API client (rest-api)
* Java client (java-client)
* Python client (python-client)
* Internal execution of Logpresso Enterprise (system)
* Internal execution of Logpresso Sonar (sonar)
* Batch Rules in Logpresso Sonar (batch-rule)
* **login\_name** (String): Login user name
* **remote\_ip** (String): Client IP address. When using a load balancer, the X-Forwarded-For header value is used.
* **rows** (64-bit integer): Number of query results. This can be monotonically increasing until the query completes.
* **elapsed** (64-bit integer): Elapsed time since query execution (in milliseconds)
* **is\_finished** (Boolean): Whether the query is finished or not
* **is\_cancelled** (Boolean): Whether the query was requested to be canceled. A query can be canceled by the user explicitly requesting it or by a failure in the command's internal operations (such as a network error). There is a time difference between the request to cancel the query and the completion of the query. There is a time difference between the query cancel request and the completion of the query.
* **is\_scheduled\_query** (Boolean): Whether the query is scheduled.
* **constants** (Map): Constant key-value list. Used when passing query parameters, such as running a procedure or scheduled query.
* **query\_string** (String): Original query string (preserved in its original form).
* **start\_time** (64-bit integer): Query start time (UNIX epoch)
* **finish\_time** (64-bit integer): Query finish time (UNIX epoch)
* **last\_started** (String): Query start time (yyyy-MM-dd HH:mm:ssZ)
* **background** (Boolean): Whether to run in the background. Foreground queries are immediately canceled when the session ends, but background queries continue to run even when the session ends.
* **commands** (Array): list of commands in the query
* **command** (String): Normalized query command
* **status** (String): Command execution status. One of the following statuses: Waiting, Running, Finalizing, or End.
* **push\_count** (64-bit integer): Number of records passed to the next command.
* **sub\_queries** (Array): List of subqueries
* **id** (32-bit integer): Query ID
* **commands** (Array): Command list
* **name** (32-bit integer): Command name
* **command** (String): Normalized query statement
* **push\_count** (64-bit integer): Number of records passed to the next command
* **status** (String): Command execution status. One of the following statuses: Waiting, Running, Finalizing, or End.
* **stamp** (32-bit integer): Query status inquiry version that is used to distinguish the latest version of a status response for the same query ID when more than one status inquiry is made by a client at the same time.
* **tags** (Map): Tag key-value list used by client to hold arbitrary, volatile, user-defined data in the query object on the Logpresso server (e.g. paging counts per query).

#### Error Responses

Query does not exist

HTTP status code 403. Query status cannot be retrieved if the query does not exist or if it was executed by a different account.

{ "error\_code": "invalid-query-id", "error\_msg": "cannot access query 42"}

Qeury ID is not an integer

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "query id should be integer type"}

### Create Cursor

Run a query in the background mode and returns the server cursor.

Be sure to delete cursors when you are done using them; any cursors that remain unused unnecessarily occupy heap memory on the Logpresso server.

#### HTTP Request

POST /api/sonar/cursors

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| q | O | String | Logpresso query statement |  |

#### Success Response

{ "id": 109 }

* **id** (32-bit integer): ID of query in background mode

#### Error Responses

Missing argument

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "q should be not null"}

Invalid query

HTTP status code 400

{ "error\_code": "invalid-query", "error\_msg": "(10200) missing-json-quotation"}

### Fetch Cursor

Fetchs the result of a specified query.

#### HTTP Request

GET /api/sonar/cursors/:id

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ "https://HOSTNAME/api/sonar/cursors/109?offset=0&limit=10"

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| id | O | 32-bit integer | Logpresso query ID |  |
| offset | X | 64-bit integer | Number of records to skip | Minumum: 0. Default: 0. |
| limit | X | 64-bit integer | Maximum number of records to load | Minimum: 0. Default: 1000. |
| format | X | String | Output format | html or xml or csv or json |

#### Success Response

Below is an example of a response from the system tables | fields table query. If format is not specified, it is returned in newline-delimited JSON format.

\{"table":"sonar\_event\_00001"}{"table":"sonar\_raw\_event\_00001"}

If you specify the offset equal to or greater than the total number of query results, nothing will be retrieved. offset value must be smaller than the rows value from [Get Query Status](https://docs.logpresso.com/en/sonar/4.0/api/get-query-status).

#### Error Responses

Failed to fetch a specified cursor

HTTP status code 403. If the query does not exist or is executed by another user account, you can't fetch the cursor.

{ "error\_code": "invalid-query-id", "error\_msg": "cannot access query 42"}

Query ID is not an integer

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "query id should be integer type"}

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "offset should be long type."}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "offset should be non-negative integer."}

Invalid format value

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "format should be html, xml, csv, or json."}

### Remove Cursor

Deletes the server cursor of a specified query ID.

#### HTTP Request

DELETE /api/sonar/cursors/:id

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| id | O | 32-bit integer | Logpresso query ID |  |

#### Success Response

{ "status": "ok"}

#### Error Responses

Query does not exist

HTTP status code 403 . If the cursor does not exist or if the query is executed by a different account, you can not delete the cursor.

{ "error\_code": "invalid-query-id", "error\_msg": "cannot access query 42"}

Query ID is not an integer

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "query id should be integer type"}

## User API

### Verify Password

Verifies login user name and password. Administrator privileges are required to call this API.

#### HTTP Request

POST /api/sonar/verify-password

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d login=xeraph \ -d password=PASSWORD \ -X POST \ https://HOSTNAME/api/sonar/verify-password

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| login | O | String | Login user name | Maximum 255 characters |
| password | O | String | Password |  |

#### Success Response

{ "status": "ok"}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "login should be not null"}

User is not found

HTTP status code 200

{ "status": "error", "reason": "user-not-found"}

passwords do not match

HTTP status code 200

{ "status": "error", "reason": "password-mismatch"}

No privileges to use authentication API

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Get Users

Gets a list of the users that match the search keyword.

#### HTTP Request

GET /api/sonar/users

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/users

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load | If not specified, load all records |
| keywords | X | String | Keyword | Search available by login, name, title, dept, phone, mobile. |
| company\_guid | X | String | Company GUID | Option only available for a cluster administrator |
| guids | X | List (of strings) | User GUID list | Comma-separated GUID list |

#### Success Response

{ "total\_count": 1, "users": [ { "guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "login": "joshua", "name": "Joshua", "title": null, "dept": null, "phone": null, "mobile": null, "email": "joshua@example.com", "locale": "ko", "role\_id": 1, "role\_name": "MASTER", "home\_menu\_id": 18, "user\_group\_guids": [], "trust\_hosts": [], "idle\_behavior": "lock", "idle\_timeout": 3600, "password\_expiration": -1, "last\_pw\_change": "2022-09-11 21:08:39+0900", "login\_lock\_count": 5, "login\_lock\_interval": 10, "login\_lock\_until": null, "login\_fail\_count": 0, "auth\_mode": 0, "has\_api\_key": true, "preferences": {}, "created": "2022-09-01 00:31:13+0900", "updated": "2022-09-11 21:08:39+0900" } ]}

* **total\_count** (32-bit integer): Total number of the user lists that match the search keyword
* **users** (Array): User list
* **guid** (String): User GUID
* **company\_guid** (String): Company GUID
* **login** (String): Login user name
* **name** (String): User name
* **title** (String): Title
* **dept** (String): Department
* **phone** (String): Phone number
* **phone** (String): Mobile number
* **email** (String): Email
* **locale** (String): Language. en or ko
* **role\_id** (32-bit integer): Role ID. Guest (0), Cluster administrator (1), Company administrator (2), User (3)
* **role\_name** (String): Role name
* **home\_menu\_id** (32-bit integer): Home menu ID to appear after login
* **user\_group\_guids** (Array): GUID list of user groups to which user belongs
* **trust\_hosts** (String): List of trusted ip addresses. If specified, access from IP addresses other than these specified ones is not allowed.
* **idle\_behavior** (String): Idle session timeout behavior. Screen lock (lock) or auto logout (logout)
* **idle\_timeout** (32-bit integer): idle session timeout time (seconds). Value ranges from 0 to 604,800 (seconds). 0 (unlimited)
* **password\_expiration** (32-bit integer): Password expiration period (in days). Value ranges from 7 to 3650. System default (-1), Unlimited (0).
* **last\_pw\_change** (String): Date and time of last password change (yyyy-MM-dd HH:mm:ssZ)
* **login\_lock\_count** (32-bit integer): Account lockout threshold. Value ranges from 0 to 5. If set to 0, account will be locked immediately upon the first authentication failure.
* **login\_lock\_interval** (32-bit integer): Account lockout duration. Min. 1 to max. 100000000 minutes.
* **login\_lock\_until** (String): Date and time of account unlock (yyyy-MM-dd HH:mm:ssZ)
* **login\_fail\_count** (32-bit integer): Number of consecutive failed login attempt
* **login\_fail\_count** (32-bit integer): Number of consecutive failed login attempts
* **auth\_mode** (32-bit integer): AAuthentication mode; 0: Use both internal/external authentication methods. 1: Use only external authentication.
* **has\_api\_key** (Boolean): Whether to have API key or not
* **preferences** (Map): Preference list
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "company\_guid should be guid type."}

### Get User

Retrieves information of a specified user.

#### HTTP Request

GET /api/sonar/users/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/users/ffaf431b-653a-4329-8f83-913cbb00342d

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | User GUID |  |

#### Success Response

{ "user": { "guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "login": "joshua", "name": "Joshua", "title": null, "dept": null, "phone": null, "mobile": null, "email": "joshua@example.com", "locale": null, "role\_id": 1, "role\_name": "MASTER", "home\_menu\_id": 18, "granted\_tables": [ { "type": "TABLE", "name": "weblog", "read\_only": true, "created": "2022-09-11 21:23:45+0900" } ], "user\_granted\_profiles": [ { "type": "PROFILE", "guid": "2011297e-6a3f-45de-92a3-8c187edb62d2", "name": "testdb (Database)", "read\_only": true, "created": "2022-09-11 21:23:45+0900" } ], "group\_granted\_profiles": [], "user\_group\_guids": ["28c1251b-2f7c-4c58-95a1-fc4a1ead877e"], "trust\_hosts": [], "idle\_behavior": "lock", "idle\_timeout": 3600, "password\_expiration": 7, "last\_pw\_change": "2022-09-11 21:08:39+0900", "login\_lock\_count": 5, "login\_lock\_interval": 10, "login\_lock\_until": null, "login\_fail\_count": 0, "auth\_mode": 0, "has\_api\_key": true, "preferences": {}, "created": "2022-09-01 00:31:13+0900", "updated": "2022-09-11 21:08:39+0900" }}

* **user** (Map): User account
* **guid** (String): User GUID
* **company\_guid** (String): Company GUID
* **login** (String): Login user name
* **name** (String): User name
* **title** (String): Title
* **dept** (String): Department
* **phone** (String): Phone number
* **mobile** (String): Mobile number
* **email** (String): Email
* **locale** (String): Locale. en or ko
* **role\_id** (32-bit integer): Role ID. Guest (0), Cluster administrator (1), Company administrator (2), User (3)
* **role\_name** (String): Role name
* **home\_menu\_id** (32-bit integer): Home menu ID to appear after login
* **granted\_tables** (Array)
* **type** (String): Always TABLE.
* **name** (String): Table name
* **read\_only** (Boolean): Whether read-only or not
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **user\_granted\_profiles** (Array)
* **type** (String): Always PROFILE.
* **guid** (String): Profile GUID
* **name** (String): Table name
* **read\_only** (Boolean): Whether read-only or not
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **group\_granted\_profiles** (Array)
* **type** (String): Always PROFILE.
* **guid** (String): Profile GUID
* **name** (String): Table name
* **read\_only** (Boolean): Whether read-only or not
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **user\_group\_guids** (Array): GUID list of user groups to which user belongs
* **trust\_hosts** (String): List of trusted ip addresses. If specified, access from IP addresses other than these specified ones is not allowed.
* **idle\_behavior** (String): Idle session timeout behavior. Screen lock (lock) or auto logout (logout)
* **idle\_timeout** (32-bit integer): Idle session timeout time (seconds). Value ranges from 0 to 604,800 (seconds). 0 (unlimited)
* **password\_expiration** (32-bit integer): Password expiration period (in days). Value ranges from 7 to 3650. System default (-1), Unlimited (0).
* **last\_pw\_change** (String): Date and time of last password change (yyyy-MM-dd HH:mm:ssZ)
* **login\_lock\_count** (32-bit integer): Account lockout threshold. Value ranges from 0 to 5. If set to 0, account will be locked immediately upon the first authentication failure.
* **login\_lock\_interval** (32-bit integer): Account lockout duration. Min. 1 to max. 100000000 minutes.
* **login\_lock\_until** (String): Date and time of account unlock (yyyy-MM-dd HH:mm:ssZ )
* **login\_fail\_count** (32-bit integer): Number of consecutive failed login attempt
* **auth\_mode** (32-bit integer): Authentication mode; 0: Use both internal/external authentication methods. 1: Use only external authentication.
* **has\_api\_key** (Boolean): Whether to have API key or not
* **preferences** (Map): Preference list
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

User Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

User is not found or No read privileges

HTTP status code 200

{ "user": null}

### Create User

Creates a new user.

#### HTTP Request

POST /api/sonar/users

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d login=jsmith \ -d role\_id=2 \ -d name="John Smith" \ -d email="john.smith@example.com" \ -d password="PASSWORD" \ -X POST \ https://HOSTNAME/api/sonar/users

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| login | O | String | Login user name | Maximum 255 characters |
| role\_id | O | 32-bit integer | Role ID | 1 or 2 or 3. Refer to the below description. |
| name | O | String | User name | Minimum 1 to maximum 50 characters |
| email | O | String | Email address | Minimum 1 to maximum 255 characters |
| password | X | String | Password | Minimum 9 characters (complying with the password policy) |
| api\_key | X | String | API key | 36 characters |
| company\_guid | X | String | Company GUID | 36 characters |
| title | X | String | Title | Maximum 20 characters |
| dept | X | String | Department | Maximum 50 characters |
| phone | X | String | Phone number | Maximum 50 characters |
| mobile | X | String | Mobile number | Maximum 50 characters |
| locale | X | String | Locale | en or ko |
| home\_menu\_id | X | 32-bit integer | Home menu ID |  |
| ticket\_repos | X | List (of strings) | Ticket repository GUID list | Comma-separated list |
| readable\_tables | X | List (of strings) | Readable table list | Comma-separated list |
| user\_group\_guids | X | List (of strings) | User group GUID list | Comma-separated list |
| trust\_hosts | X | List (of strings) | Trusted IPs | Comma-separated list |
| idle\_behavior | X | String | Idle session timeout behavior | lock or logout |
| idle\_timeout | X | 32-bit integer | Idle session timeout time (in seconds) | Minimum 60 to maximum 604800. Default: 600 |
| password\_expiration | X | 32-bit integer | Password expiration period (days) | System default: -1, Unlimited: 0, Minimum 7 to maximum 3650 |
| login\_lock\_count | X | 32-bit integer | Account lockout threshold | Minimum 0 to maximum 5 (Default: 5) |
| login\_lock\_interval | X | 32-bit integer | Account lockout duration (minutes) | Minimum 1 to maximum 100000000 (Default: 10) |
| auth\_mode | X | 32-bit integer | Authentication mode | 0: Use both internal/external authentication methods (default). 1: Use only external authentication. |

**Role ID**

* (1) Cluster administrator: User with all privileges including cluster administrator privileges.
* (2) Company administrator: User with tenant privileges.
* (3) User: User with privileges to edit and view user objects such as dashboards, widgets, datasets, and tickets.

**Password policy**

* Minimum 9 characters.
* Alphanumeric characters and special characters must be included.
* Any three identical consecutive characters are not allowed.

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "login should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'login' must be shorter than or equal to 255 characters."}

Company identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "company\_guid should be guid type."}

Duplicate login user name

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "duplicate-login"}

Invalid email format

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'email' parameter is not a valid email address: foo"}

No password specified for password authentication mode

HTTP status code 400. Password must be entered if auth\_mode is not specified or set to 0.

{ "error\_code": "null-argument", "error\_msg": "password should be not null"}

Insufficient password complexity

HTTP status code 400. Password should not contain login user name.

{ "error\_code": "invalid-argument", "error\_msg": "password contains login name"}

HTTP status code 400. The password does not consist of a combination of alphanumeric characters and special characters.

{ "error\_code": "invalid-argument", "error\_msg": "password should contain digits, alphabets, and special characters"}

HTTP status code 400. The password contains three consecutive identical characters.

{ "error\_code": "invalid-argument", "error\_msg": "password should not repeat same characters"}

Locale is not supported

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "unsupported locale: ru"}

Role ID is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "unknown role id: 5"}

Menu ID is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "unknown menu id: 0"}

Invalid authentication mode

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "auth\_mode should be 0 or 1. input is 2."}

Create a user with higher privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no permission: cannot create cluster admin by user"}

User group is not found or available

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "user group not found: 28c1251b-2f7c-4c58-95a1-fc4a1ead877e"}

### Update User

Updates a specified user.

#### HTTP Request

PUT /api/sonar/users/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d login=jsmith \ -d role\_id=2 \ -d name="John Smith" \ -d idle\_behavior=lock \ -d idle\_timeout=600 \ -d email="john.smith@example.com" \ -X PUT \ https://HOSTNAME/api/sonar/users/bfd00bb0-be99-4fd5-8380-166f544975fa

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | User GUID | 36 characters |
| login | O | String | Login user name | Maximum 255 characters |
| role\_id | O | 32-bit integer | Role ID | 1 or 2 or 3. Refer to the description below. |
| name | O | String | User name | Minimum 1 to maximum 50 characters |
| email | O | String | Email address | Minimum 1 to maximum 255 characters |
| password | X | String | Password | Minimum 9 characters (Complying with the password policy). If not specified, the existing password is used. |
| api\_key | X | String | API Key | 36 characters long GUID. If not specified, the existing API key is used. |
| company\_guid | X | String | Company GUID | 36 characters long GUID. If not specified, the existing company GUID is used. |
| title | X | String | Job title | Maximum 20 characters. If not specified, the existing value is deleted. |
| dept | X | String | Department | Maximum 50 characters. If not specified, the existing value is deleted. |
| phone | X | String | Phone number | Maximum 50 characters. If not specified, the existing value is deleted. |
| mobile | X | String | Mobile number | Maximum 50 characters. If not specified, the existing value is deleted. |
| locale | X | String | Locale | en or ko. If not specified, the locale of the session is applied. |
| home\_menu\_id | X | 32-bit integer | Home menu ID | If not specified, the existing value is deleted. |
| ticket\_repos | X | List (of strings) | Ticket repository GUID list | Comma-separated list. If not specified, the existing value is deleted. |
| readable\_tables | X | List (of strings) | Readable table name list | Comma-separated list. If not specified, the existing value is deleted. |
| user\_group\_guids | X | List (of strings) | User group GUID list | Comma-separated list. If not specified, the existing value is deleted. |
| trust\_hosts | X | List (of strings) | Trusted IP list | Comma-separated list. If not specified, the existing value is deleted. |
| idle\_behavior | X | String | Idle session timeout behavior | lock or logout. If not specified, the existing value is deleted. |
| idle\_timeout | X | 32-bit integer | Idle session timeout time (seconds) | Minimum 60 to maximum 604800. Default: 600 |
| password\_expiration | X | 32-bit integer | Password expiration period (days) | System default (-1), Unlimited (0), Minimum 7to maximum 3650. |
| login\_lock\_count | X | 32-bit integer | Account lockout threshold | Minimum 0 to maximum 5. Default: 5 |
| login\_lock\_interval | X | 32-bit integer | Account lockout duration (in minutes) | Minimum 1 to maximum 100000000. Default: 10 |
| auth\_mode | X | 32-bit integer | Authentication mode | 0: Use both internal/external authentication methods (default). 1: Use only external authentication. |

**Role ID**

* (1) Cluster administrator: User with all privileges including cluster administrator privileges.
* (2) Company administrator: User with tenant privileges.
* (3) User: User with privileges to manage user objects such as dashboards, widgets, datasets, and tickets.

**Password Policy**

* Minimum 9 characters.
* Alphanumeric characters and special characters must be included.
* Any three identical consecutive characters are not allowed.

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "login should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'login' must be shorter than or equal to 255 characters."}

User identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Duplicate login user name

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "duplicate-login"}

Invalid email format

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'email' parameter is not a valid email address: foo"}

No password specified for password authentication mode

HTTP status code 400. Password must be entered if auth\_mode is not specified or set to 0.

{ "error\_code": "null-argument", "error\_msg": "password should be not null"}

Insufficient password complexity

HTTP status code 400. Password should not contain login user name.

{ "error\_code": "invalid-argument", "error\_msg": "password contains login name"}

HTTP status code 400. The password does not consist of a combination of alphanumeric characters and special characters.

{ "error\_code": "invalid-argument", "error\_msg": "password should contain digits, alphabets, and special characters"}

HTTP status code 400. The password contains three consecutive identical characters.

{ "error\_code": "invalid-argument", "error\_msg": "password should not repeat same characters"}

Locale is not supported

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "unsupported locale: ru"}

Role ID is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "unknown role id: 5"}

Menu ID is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "unknown menu id: 0"}

Invalid authentication mode

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "auth\_mode should be 0 or 1. input is 2."}

Update a user with higher privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

Update own role

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "cannot update role by yourself."}

User group is not found or available

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "user group not found: 28c1251b-2f7c-4c58-95a1-fc4a1ead877e"}

### Remove Users

Deletes the specified users.

#### HTTP Request

DELETE /api/sonar/users

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/users?guids=6ba6031e-9d03-4a2b-8372-20ceee8f2a76"

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guids | O | String | User identifier list | Comma-separated list |

#### Success Response

{ "failures": []}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "guids should be not null"}

User Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

Delete a user with higher privileges

HTTP status code 200

{ "failures": [ { "guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "login": "xeraph" "name": "Yang BongYeol", "reason": "no-permission", } ]}

Delete own account

HTTP status code 200

{ "failures": [ { "guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "login": "xeraph" "name": "Yang BongYeol", "reason": "cannnot-remove-yourself", } ]}

User is not found

HTTP status code 200. The same error response is returned when a non-cluster administrator attempts to delete an account that belongs to another company (tenant).

{ "failures": [ { "guid": "6ba6031e-9d03-4a2b-8372-20ceee8f2a75" "reason": "user-not-found", } ]}

## User Group API

### Get User Groups

Get a list of the user groups that match the search keyword.

#### HTTP Request

GET /api/sonar/user-groups

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/user-groups

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load | If not specified, load all records |
| keywords | X | String | Keyword | Search available by name, description |
| company\_guid | X | String | Company GUID | Option only available for a cluster administrator |
| guids | X | List (of strings) | User group GUID list | Comma-separated list |

#### Success Response

{ "total\_count": 1, "user\_groups": [ { "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "guid": "28c1251b-2f7c-4c58-95a1-fc4a1ead877e", "name": "Cyber Security", "description": "", "owner\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "owner\_name": "Yang", "created": "2022-09-01 01:08:00+0900", "updated": "2022-09-01 01:08:00+0900" } ]}

* **total\_count** (32-bit integer): Total number of the user groups that match the search keyword
* **groups** (Array): User group list
* **company\_guid** (String): Company (tenant) GUID
* **company\_name** (String): Company (tenant) name
* **guid** (String): User group GUID
* **name** (String): User group name
* **description** (String): Description
* **owner\_guid** (String): GUID of the user who creates the user group
* **owner\_name** (String): Name of the user who creates the user group
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### Get User Group

Retrieves information of a specified user group.

#### HTTP Request

GET /api/sonar/user-groups/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/user-groups/28c1251b-2f7c-4c58-95a1-fc4a1ead877e

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | User group GUID | 36 characters |

#### Success Response

{ "user\_group": { "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "guid": "28c1251b-2f7c-4c58-95a1-fc4a1ead877e", "name": "Cyber Security", "description": "", "owner\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "owner\_name": "Yang", "user\_guids": ["ffaf431b-653a-4329-8f83-913cbb00342d"], "created": "2022-09-01 01:08:00+0900", "updated": "2022-09-01 01:08:00+0900" }}

* **total\_count** (32-bit integer): Total number of the user groups that match the search keyword
* **groups** (Array): User group list
* **company\_guid** (String): Company (tenant) GUID
* **company\_name** (String): Company (tenant) name
* **guid** (String): User group GUID
* **name** (String): User group name
* **description** (String): Description
* **owner\_guid** (String): GUID of the user who creates the user group
* **owner\_name** (String): Name of the user who creates the user group
* **user\_guids** (Array): List of the GUIDs for users in the user group
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

User group cannot be retrieved

HTTP status code 200

{ "user\_group": null}

### Create User Group

Creates a new user group.

#### HTTP Request

POST /api/sonar/user-groups

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="Cyber Security" \ -X POST \ https://HOSTNAME/api/sonar/user-groups

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| name | O | String | User group name | Minimum 1 to maximum 200 characters |
| guid | X | String | User group GUID | 36 characters |
| company\_guid | X | String | Company GUID | 36 characters. Option only available for a cluster administrator |
| description | X | String | Description | Maximum 2,000 characters |
| user\_guids | X | Array | User identifier group | Invalid user identifier is ignored. |

#### Success Response

{}

#### Error Responses

Required argument is missing

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Invalid argument length

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be shorter than or equal to 200 characters."}

User identifier is not in valid GUID format

{ "error\_code": "invalid-param-type", "error\_msg": "user\_guids should be guid type."}

### Update User Group

Updates a specified user group.

#### HTTP Request

PUT /api/sonar/user-groups/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="Cyber Security" \ -d user\_guids=ffaf431b-653a-4329-8f83-913cbb00342d \ -X PUT \ https://HOSTNAME/api/sonar/user-groups/a2a42968-787f-45a3-bec9-b6b68db21c2f

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| name | O | String | User group name | Minimum 1 to maximum 200 characters |
| guid | X | String | User group GUID | 36 characters |
| description | X | String | Description | Maximum 2,000 characters |
| user\_guids | X | Array | List of user GUIDs | Invalid user GUID is ignored |

#### Success Response

{}

#### Error Responses

Required argument is missing

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Invalid argument length

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be shorter than or equal to 200 characters."}

User identifier is not in valid GUID format

{ "error\_code": "invalid-param-type", "error\_msg": "user\_guids should be guid type."}

User group is not found

An inquiry failure response is returned when a non-cluster administrator attempts to delete an account that belongs to another company (tenant).

{ "error\_code": "illegal-state", "error\_msg": "user group not found: a2a42968-787f-45a3-bec9-b6b68db21c2d"}

### Remove User Groups

Deletes the specified user groups.

#### HTTP Request

DELETE /api/sonar/user-groups

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/user-groups?guids=a2a42968-787f-45a3-bec9-b6b68db21c2f"

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guids | O | String | User group GUID list | Comma-separated list |

#### Success Response

{}

#### Error Responses

Required argument is missing

{ "error\_code": "null-argument", "error\_msg": "guids should be not null"}

Identifier is not in valid GUID format

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

No privileges to delete a user group

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## Connect Profile API

### Get Connect Profile Types

Gets a list of available connect profile types.

#### HTTP Request

GET /api/sonar/connect-profile-types

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/connect-profile-types

#### Success Response

The example below shows the types of connect profiles built into the default package. The list of connect profiles is dynamically expanded when you install a new app.

{ "profile\_factories": [ { "type": "ftp", "name": "FTP", "description": "Manage FTP connect profiles." }, { "type": "ldap", "name": "LDAP", "description": "Manage LDAP connect profiles." }, { "type": "ssh", "name": "SSH", "description": "Manage SSH connect profiles." }, { "type": "taxii", "name": "TAXII", "description": "Manage connection properties for TAXII 2.0" }, { "type": "jdbc", "name": "Database", "description": "Manage JDBC driver connection strings" }, { "type": "mongo", "name": "MongoDB", "description": "Manage MongoDB connect profiles." } ]}

* **profile\_factories** (Array): List of connect profile types
* **type** (String): Connect profile type identifier
* **name** (String): Connect profile type name
* **description** (String): Connect profile type description

### Get Connect Profile Options

Retrieves option specification for a specified connect profile type.

#### HTTP Request

GET /api/sonar/connect-profile-types/:type/options

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/connect-profile-types/ssh/options

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| type | O | String | Connect profile type identifier |  |

#### Success Response

{ "options": [ { "type": "string", "subtype": "connection-string", "name": "connection\_string", "required": true, "display\_name": "Connection String", "description": "", "default\_value": null, "protected": false }, { "type": "string", "subtype": null, "name": "user", "required": false, "display\_name": "User", "description": "", "default\_value": null, "protected": false }, { "type": "string", "subtype": null, "name": "password", "required": false, "display\_name": "Password", "description": "", "default\_value": null, "protected": true }, { "type": "boolean", "subtype": null, "name": "read\_only", "required": false, "display\_name": "Read Only", "description": "Read Only", "default\_value": "false", "protected": false } ]}

* **options** (Array): List of options
* **type** (String): Data type. One of the following: string, integer, boolean.
* **subtype** (String): Extension component type in the UI
* **name** (String): Option key
* **required** (Boolean): whether the option is required or not
* **display\_name** (String): Display name in locale language
* **description** (String): Description in locale language
* **default\_value** (String): Default value to display on screen
* **protected** (Boolean): Whether protected or not. Set to true for options like "password" that should not be visible when retrieving the profile.

#### Error Responses

Profile type does not exist

{ "options": null}

### Get Connect Profiles

Gets a list of available connect profiles.

#### HTTP Request

GET /api/sonar/connect-profiles

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ "https://HOSTNAME/api/sonar/connect-profiles?offset=0&limit=20"

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load | Default: 2147483647 |
| type | X | String | Connect profile type | Search only by a specified profile type |
| keywords | X | String | Keyword | Search available by code, name, description |
| company\_guid | X | String | Company GUID | Option only available for a cluster administrator |

#### Success Response

{ "total\_count": 1, "profiles": [ { "guid": "b7f00412-8720-4a8f-ac35-7d7f359f797e", "code": "build", "name": "Build SSH", "type": "ssh", "description": "", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "configs": { "password": "", "port": 22, "host": "build", "server\_alive\_interval": null, "user": "logpresso", "timeout": 30 }, "config\_description": "Host: build, Port: 22, User: xeraph, Auth Method: Password, Timeout: 30 secs", "factory\_display\_name": "SSH", "created": "2022-09-01 00:39:35+0900", "updated": "2022-09-01 00:39:35+0900", "grant\_users": [ { "type": "USER", "guid": "bfd00bb0-be99-4fd5-8380-166f544975fa", "name": "Joshua", "read\_only": true, "created": "2022-09-02 19:38:21+0900" } ], "grant\_groups": [ { "type": "USER", "guid": "28c1251b-2f7c-4c58-95a1-fc4a1ead877e", "name": "dev", "read\_only": true, "created": "2022-09-02 19:38:21+0900" } ], "protected\_keys": ["password"] } ]}

* **total\_count** (32-bit integer): Total number of the connect profiles that match the specified search keyword
* **profiles** (Array): List of the connect profiles that match the specified search keyword
* **guid** (String): Connect profile GUID
* **code** (String): Code for query. Unique name among same connect profile type.
* **name** (String): Display name of the connect profile
* **type** (String): Connect profile type
* **description** (String): Connect profile description
* **company\_guid** (String): GUID of the company to which the connect profile belongs
* **company\_name** (String): Name of the company to which the connect profile belongs
* **configs** (Map): Connect profile Key/value pairs. Protected options, like password, do not return the original value, but rather an empty string indicating that they are set.
* **config\_description** (String): Connect profile option summary. Key information to identify a specific connect profile in the list.
* **factory\_display\_name** (String): Display name of the connect profile. For example, the jdbc type returns database in Korean.
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)
* **grant\_users** (Array): List of the users authorized to use connect profiles
* **type** (String): Common object type. Always USER.
* **guid** (String): User GUID
* **name** (String): User name
* **read\_only** (Boolean): Whether read-only or not. Always false.
* **created** (String): Date and time when privilege mappings are generated
* **grant\_groups** (Array): List of user groups with privilege for the connect profile
* **type** (String): Common object type. Always USER.
* **guid** (String): User group GUID
* **name** (String): User group name
* **read\_only** (Boolean): Whether read-only or not. Always false.
* **created** (String): Date and time when privilege mappings are generated
* **protected\_keys** (Array): List of the protected option key names. For example, the password setting is not returned because it is protected.

#### Error Responses

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "company\_guid should be guid type."}

### Get Connect Profile

Retrieves information of a specified connect profile.

#### HTTP Request

GET /api/sonar/connect-profiles/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/connect-profiles/b7f00412-8720-4a8f-ac35-7d7f359f797e

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Connect profile GUID |  |

#### Success Response

{ "profile": { "guid": "b7f00412-8720-4a8f-ac35-7d7f359f797e", "code": "build", "name": "Build SSH", "type": "ssh", "description": "", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "configs": { "password": "", "port": 22, "host": "build", "server\_alive\_interval": null, "user": "logpresso", "timeout": 30 }, "config\_description": "Host: build, Port: 22, User: xeraph, Auth Method: Password, Timeout: 30 secs", "factory\_display\_name": "SSH", "created": "2022-09-01 00:39:35+0900", "updated": "2022-09-01 00:39:35+0900", "grant\_users": [ { "type": "USER", "guid": "bfd00bb0-be99-4fd5-8380-166f544975fa", "name": "Joshua", "read\_only": true, "created": "2022-09-02 19:38:21+0900" } ], "grant\_groups": [ { "type": "USER", "guid": "28c1251b-2f7c-4c58-95a1-fc4a1ead877e", "name": "dev", "read\_only": true, "created": "2022-09-02 19:38:21+0900" } ], "protected\_keys": ["password"] }}

* **profile** (Map): Specified connect profile
* **guid** (String): Connect profile GUID
* **code** (String): Code for query. Unique name among same connect profile type.
* **name** (String): Display name of the connect profile
* **type** (String): Connect profile type
* **description** (String): Connect profile description
* **company\_guid** (String): GUID of the company to which the connect profile belongs
* **company\_name** (String): Name of the company to which the connect profile belongs
* **configs** (Map): Connect profile Key/value pairs. Protected options, like password, do not return the original value, but rather an empty string indicating that they are set.
* **config\_description** (String): Connect profile option summary. Key information to identify a specific connect profile in the list.
* **factory\_display\_name** (String): Display name of the connect profile. For example, the jdbc type returns database in Korean.
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)
* **grant\_users** (Array): List of users with privileges for the connect profile
* **type** (String): Common object type. Always USER.
* **guid** (String): User GUID
* **name** (String): User name
* **read\_only** (Boolean): Whether read-only or not. Always false.
* **created** (String): Date and time when privilege mappings are generated
* **grant\_groups** (Array): List of user groups with privileges for the connect profile
* **type** (String): Common object type. Always USER.
* **guid** (String): User group identifier
* **name** (String): User group name
* **read\_only** (Boolean): Whether read-only or not. Always false.
* **created** (String): Date and time when privilege mappings are generated
* **protected\_keys** (Array): List of the protected option key names. For example, the password setting is not returned because it is protected.

#### Error Responses

Identifier is not in valid GUID format

{ "error\_code": "invalid-argument", "error\_msg": "Invalid UUID string: invalid"}

Connect profile does not exist

{ "profile": null}

### Create Connect Profile

Creates a new connect profile.

#### HTTP Request

POST /api/sonar/connect-profiles

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d company\_guid=6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311 \ -d code=testdb \ -d type=jdbc \ -d name="Hyper SQL" \ -d description="Embedded file database" \ -d configs="{""connection\_string"":""jdbc:hsqldb:file:testdb"", ""user"":""SA"", ""password"":null, ""read\_only"":false}" \ -X POST \ https://HOSTNAME/api/sonar/connect-profiles

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| company\_guid | X | String | Company GUID | 36 characters. The default is the GUID of the company in the current session. |
| guid | X | String | Connect profile GUID | 36 characters. The default is randomly generated. |
| code | O | String | Connect profile name | Minimum 1 to maximum 50 characters |
| type | O | String | Connect profile type | E.g. jdbc |
| name | O | String | Connect profile display name | Minimum 1 to maximum 50 characters |
| description | X | String | Connect profile Description | Maximum 2,000 characters |
| grant\_users | X | String | GUID list of the users with privileges for the profile | Comma-separated list |
| grant\_groups | X | String | GUID list of the user groups with privileges for the profile | Comma-separated list |
| configs | O | String key/value | Configuration | JSON format String |

The connect profile name (code) is used as the name referenced in queries, such as the `parse` command.

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "code should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

Missing required configuration option value

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "config option must be not null: connection\_string"}

Invalid connect profile type

HTTP status code 400

{ "error\_code": "unknown-profile-type", "error\_msg": null}

Duplicate connect profile name

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "duplicate-code: testdb"}

Invalid company GUID

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "invalid-company-guid: 1fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311"}

No privilege to manage the company

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Update Connect Profile

Updates a specified connect profile.

#### HTTP Request

PUT /api/sonar/connect-profiles/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="Hyper SQL" \ -d description="Embedded file database" \ -d configs="{""connection\_string"":""jdbc:hsqldb:file:testdb"", ""user"":""SA"", ""password"":""NEW\_PASSWORD"", ""read\_only"":false, ""update\_keys"": [""password""]}" \ -X PUT \ https://HOSTNAME/api/sonar/connect-profiles/b7f00412-8720-4a8f-ac35-7d7f359f797e

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Connect profile GUID | 36 characters |
| name | O | String | Display name of the connect profile | Minimum 1 to maximum 50 characters |
| description | X | String | Connect profile description | Maximum 2,000 characters |
| grant\_users | X | String | GUID list of the users with privileges | Comma-separated list |
| grant\_groups | X | String | GUID list of the user groups with privileges | Comma-separated list |
| configs | O | String key/value | Configuration values. Refer to the below description. | JSON format string |

If you do not include protected configuration keys in the configs parameter when requesting a connect profile modification, the previous configuration values are retained. To update a protected configuration key with a new value, the key/value pair in the configs parameter must include the update\_keys key and a list of protected key names.

Without the update\_keys, it is unable to distinguish whether you are sending null to keep an existing configuration value or to delete an existing configuration value.

#### Success Response

{}

#### Error Responses

Connect profile is not found

{ "error\_code": "profile-not-found", "error\_msg": null}

Required argument is missing

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Invalid argument length

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

Missing required configuration value

{ "error\_code": "invalid-argument", "error\_msg": "config option must be not null: connection\_string"}

No privileges to manage the company

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Remove Connect Profiles

Deletes the specified connect profiles. If a connect profile matching the provided GUID does not exist, or if you do not have administrative privileges on that connect profile, the delete request is ignored.

#### HTTP Request

DELETE /api/sonar/connect-profiles

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/connect-profiles?guids=b7f00412-8720-4a8f-ac35-7d7f359f797e,77e0aa85-14d3-43a9-ab23-4dc97dfc185e"

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guids | O | String | Connect profile GUID list | Comma-separated list |

#### Success Response

{}

#### Error Response

Invalid GUID format

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

### Get SSH Public Key

Retrieves the Logpresso SSH public key. You can register Logpresso SSH public key to the authorized\_keys file on another system for SSH key-based authentication.

#### HTTP Request

GET /api/sonar/ssh-public-key

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/ssh-public-key

#### Success Response

{ "public\_key": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQC9w0vWHeB/HFXPXM4lTwXALyiatCGtSAoenfyJsrl63uZGU7Xji9Iz/pJJ6t5tWYz7mm2Frg9JjGq2p42xW525FgjRtIhyiPiT7/ZT80GG79Fi1wUE+BlIzXKwmfNxHxaBoW7UcPp1gMSmEycIVU/4b79JM1jfCpfPr+mq9XYzYw== "}

* **public\_key** (String): SSH public key

### Renew SSH Public Key

Deletes the old Logpresso SSH public key and generates a new one. This will invalidate Logpresso SSH key-based authentication on all systems you were previously connected to, and you will need to re-register the public key. This operation is irreversible. You need cluster administrator privileges to call this API.

#### HTTP Request

POST /api/sonar/renew-ssh-public-key

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/renew-ssh-public-key

#### Success Response

{ "public\_key": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQCjU/Fx6gogfQDS+egS2ym1c0yill9UkVxZuxpRBqSvh6/xPV24aXaFEywkYCJ0ZJkRyvyJl2FDnyO0ghu9cTRdkNWo+nlHD+LiIbAmglVLOde0I85BLVclXu2HqT8Fd4TIWmUUiIYa1adA96B8qprqKKMCLQwZSqDSNzyRG0/AvQ== "}

* **public\_key** (String): Newly generated SSH public key

#### Error Response

No cluster administrator privileges

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## Parser API

### Get Parser Factories

Get a list of parser factories.

#### HTTP Request

GET /api/sonar/parser-factories

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/parser-factories

#### Success Response

Below is an example of the parser factory list. The available parser types dynamically expand as you install a new app.

{ "groups": ["Syslog", "General", "Script", "SNMP", "File"], "factories": [ { "name": "cef", "display\_name": "CEF", "display\_group": "General", "description": "Parse CEF (Common Event Format) logs.", "options": [], "deprecated": false }, { "name": "csv", "display\_name": "CSV", "display\_group": "General", "description": "Divide a string into tokens based on the csv format and column names.", "options": [ { "type": "string", "subtype": null, "name": "use\_tab", "required": false, "display\_name": "Use tab", "description": "Use tab to delimiter. (true or false)", "default\_value": null }, { "type": "string", "subtype": null, "name": "use\_double\_quote", "required": false, "display\_name": "Double quote escape", "description": "Use double quote to escape. (true or false)", "default\_value": null }, { "type": "string", "subtype": null, "name": "column\_headers", "required": false, "display\_name": "Column headers", "description": "Column headers", "default\_value": null }, { "type": "string", "subtype": null, "name": "target\_field", "required": false, "display\_name": "Target field", "description": "Target field name", "default\_value": null }, { "type": "string", "subtype": null, "name": "include\_target", "required": false, "display\_name": "Include target", "description": "Return also target field (true or false)", "default\_value": null } ], "deprecated": false }, { "name": "json", "display\_name": "JSON", "display\_group": "General", "description": "Parse JSON format.", "options": [ { "type": "string", "subtype": null, "name": "target\_field", "required": false, "display\_name": "Target field", "description": "Target field name", "default\_value": null }, { "type": "string", "subtype": null, "name": "include\_target", "required": false, "display\_name": "Include target", "description": "Return also target field (true or false)", "default\_value": null } ], "deprecated": false }, { "name": "leef", "display\_name": "LEEF", "display\_group": "Syslog", "description": "Parse LEEF logs.", "options": [], "deprecated": false }, { "name": "welf", "display\_name": "WELF Format", "display\_group": "General", "description": "Parse WELF (WebTrends Enhanced Log Format) logs.", "options": [], "deprecated": false }, { "name": "delimiter", "display\_name": "Delimiter", "display\_group": "General", "description": "Divide a string into tokens based on the given delimiter and column names.", "options": [ { "type": "string", "subtype": null, "name": "delimiter", "required": true, "display\_name": "Delimiter", "description": "One delimiter character or 4-digit unicode escape sequence (e.g. \\u0007)", "default\_value": null }, { "type": "string", "subtype": null, "name": "column\_headers", "required": false, "display\_name": "Column headers", "description": "Separated by comma", "default\_value": null }, { "type": "string", "subtype": null, "name": "delimiter\_target", "required": false, "display\_name": "Delimiter target field", "description": "Delimiter target field name", "default\_value": null }, { "type": "string", "subtype": null, "name": "include\_delimiter\_target", "required": false, "display\_name": "Include delimiter target", "description": "Return also delimiter target field (true or false)", "default\_value": null } ], "deprecated": false }, { "name": "groovy", "display\_name": "Groovy", "display\_group": "Script", "description": "Groovy parser script", "options": [ { "type": "string", "subtype": null, "name": "script\_name", "required": true, "display\_name": "Script Name", "description": "Script file name except .groovy extension", "default\_value": null } ], "deprecated": false }, { "name": "regex", "display\_name": "Regular Expression", "display\_group": "General", "description": "Parse logs using regular expression.", "options": [ { "type": "string", "subtype": null, "name": "regex", "required": true, "display\_name": "Regex", "description": "Regular expression with placeholder.", "default\_value": null }, { "type": "string", "subtype": null, "name": "field", "required": false, "display\_name": "Target field", "description": "Parse target field. 'line' field by default.", "default\_value": null }, { "type": "string", "subtype": null, "name": "include\_original\_field", "required": false, "display\_name": "Include original field", "description": "Include original field", "default\_value": null } ], "deprecated": false }, { "name": "query", "display\_name": "Query based parser", "display\_group": "General", "description": "Parse logs using query.", "options": [ { "type": "string", "subtype": null, "name": "query", "required": true, "display\_name": "Query string", "description": "Query string for log parsing", "default\_value": null } ], "deprecated": false } ]}

* **groups** (Array): List of parser group names
* **factories** (Array): List of parser factories
* **name** (String): Parser factory name
* **display\_name** (String): Display name of the parser factory
* **display\_group** (String): Display group of parser factory
* **description** (String): Parser factory description
* **options** (Array): Option details
* **type** (String): Data type. one of the following: string, integer, boolean.
* **subtype** (String): Extension component type in the UI
* **name** (String): Configuration option key name
* **required** (Boolean): Whether the option is required or not
* **display\_name** (String): Display name in locale language
* **description** (String): Description in locale language
* **default\_value** (String): Default value to display on screen
* **deprecated** (Boolean): Whether to be deprecated or not. If a parser factory was set to "deprecated" in a previous version, it is only available with the existing settings and cannot be modified.

### Get Parser Factory

Retrieves information of a specified parser factory.

#### HTTP Request

GET /api/sonar/parser-factories/:name

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ "https://HOSTNAME/api/sonar/parser-factories/regex?locale=ko"

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| name | O | String | Parser factory name |  |
| locale | X | String | Locale | en or ko |

#### Success Response

Below is the example of retrieving regular expression parser factory.

{ "factory": { "name": "regex", "display\_name": "Regular Expression", "display\_group": "General", "description": "Parse logs using regular expression.", "deprecated": false, "options": [ { "type": "string", "subtype": null, "name": "regex", "required": true, "display\_name": "Regex", "description": "Regular expression with placeholder.", "default\_value": null }, { "type": "string", "subtype": null, "name": "field", "required": false, "display\_name": "Target field", "description": "Parse target field. 'line' field by default.", "default\_value": null }, { "type": "string", "subtype": null, "name": "include\_original\_field", "required": false, "display\_name": "Include original field", "description": "Include original field", "default\_value": null } ] }}

* **groups** (Array): List of parser group names
* **factories** (Array): List of parser factories
* **name** (String): Parser factory name
* **display\_name** (String): Display name of the parser factory
* **display\_group** (String): Display group of the parser factory
* **description** (String): Parser factory description
* **options** (Array): Option details
* **type** (String): Data type. One of the following: string, integer, boolean.
* **subtype** (String): Extension component type in the UI
* **name** (String): Option Key name
* **required** (Boolean): Whether required or not
* **display\_name** (String): Display name in locale language
* **description** (String): Description in locale language
* **default\_value** (String): Default value to display on screen
* **deprecated** (Boolean): Whether to be deprecated or not. If a parser factory was set to "deprecated" in a previous version, it is only available with the existing settings and cannot be modified.

### Get Parsers

Gets a list of the parsers that match the search keyword.

#### HTTP Request

GET /api/sonar/parsers

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/parsers

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load |  |
| type | X | String | Parser type | parser or normalizer |
| keywords | X | String | Keyword | Search available by code, name |

#### Success Response

{ "total\_count": 27, "parsers": [ { "code": "fortigate", "name": "Fortigate", "description": "Parse Fortigate logs.", "factory\_name": "fortigate", "factory\_display\_name": "Fortigate", "builtin": true, "configs": { "ver": "2" }, "created": "2022-09-01 00:31:14+0900", "updated": "2022-09-01 00:31:14+0900" } ]}

* **total\_count** (32-bit integer): Total number of parsers that match the search keyword
* **parsers** (Array): Parser list
* **code** (String): Parser code, referenced when calling the parser from the [parse command](https://docs.logpresso.com/en/sonar/4.0/api/ko/query/parse-command).
* **name** (String): Display name of the parser
* **description** (String): Parser description
* **factory\_name** (String): [Parser factory name](https://docs.logpresso.com/en/sonar/4.0/api/get-parser-factories)
* **factory\_display\_name** (String): Display name of parser type
* **builtin** (Boolean): Whether the parser is built-in in the package
* **schema\_code** (String): Log schema code. (Only for log normalizers)
* **schema\_name** (String): Display name of the log schema. (Only for log normalizers)
* **configs** (Map): List of key/value pairs in the [Parser factory information](https://docs.logpresso.com/en/sonar/4.0/api/get-parser-factory).
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

Invalid parser type

{ "error\_code": "invalid-argument", "error\_msg": "type should be 'parser' or 'normalizer': unknown"}

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### Get Parser

Retrieves information of a specified parser.

#### HTTP Request

GET /api/sonar/parsers/:code

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/parsers/fortigate

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| code | O | String | Parser code |  |

#### Success Response

{ "parser": { "code": "fortigate", "name": "Fortigate", "description": "Parse Fortigate logs.", "factory\_name": "fortigate", "factory\_display\_name": "Fortigate", "builtin": true, "configs": { "ver": "2" }, "created": "2022-09-01 00:31:14+0900", "updated": "2022-09-01 00:31:14+0900" }}

* **parser** (Map): Parser information
* **code** (String): Parser code, referenced when calling the parser from the [parse command](https://docs.logpresso.com/en/sonar/4.0/api/ko/query/parse-command).
* **name** (String): Display name of the parser
* **description** (String): Parser description
* **factory\_name** (String): [Parser factory name](https://docs.logpresso.com/en/sonar/4.0/api/get-parser-factories)
* **factory\_display\_name** (String): Display name of parser type
* **builtin** (Boolean): Whether the parser is built-in in the package
* **schema\_code** (String): Log schema code. (Only for log normalizers)
* **schema\_name** (String): Display name of the log schema. (Only for log normalizers)
* **configs** (Map): List of key/value pairs in the [Parser factory information](https://docs.logpresso.com/en/sonar/4.0/api/get-parser-factory).
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)

#### Error Response

HTTP status code 200

Parser is not found

{ "parser": null}

### Create Parser

Create a new parser. Cluster administrator privileges are required to call this API.

#### HTTP Request

POST /api/sonar/parsers

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d code=test \ -d name=Test \ -d factory\_name=fortigate \ -d configs="{""ver"":""2""}" \ -X POST \ https://HOSTNAME/api/sonar/parsers

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| code | O | String | Parser code | Minumum 1 to maximum 50 characters |
| name | O | String | Parser display name | Minumum 1 to maximum 50 characters |
| factory\_name | O | String | Parser factory name |  |
| description | X | String | Parser description | Maximum 2,000 characters |
| schema\_code | X | String | Log schema code |  |
| configs | X | String key/value | list of configuration options | JSON format string |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "code should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'code' must be less than or equal to 50 characters."}

Duplicate parser code or name

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "duplicated parser: foo"}

Parser factory is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "parser factory not found: unknown"}

Schema is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "schema not found: unknown"}

Invalid configuration value

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "parser config [query] should be not null"}

### Update Parser

Updates an existing parser. Cluster administrator privileges are required to call this API.

#### HTTP Request

PUT /api/sonar/parsers/:code

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name=Test \ -d factory\_name=fortigate \ -d configs="{""ver"":""1""}" \ -X PUT \ https://HOSTNAME/api/sonar/parsers/test

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| code | O | String | Parser code | Minimum 1 to maximum 50 characters |
| name | O | String | Display name of the parser | Minimum 1 to maximum 50 characters |
| factory\_name | O | String | Parser factory name |  |
| description | X | String | Parser description | Maximum 2,000 characters |
| schema\_code | X | String | Log schema code |  |
| configs | X | String key/value | list of configurations | JSON format String |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

Parser is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "parser not found: unknown"}

Parser factory is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "parser factory not found: unknown"}

Schema is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "schema not found: unknown"}

Invalid configuration value

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "parser config [query] should be not null"}

### Remove Parsers

Deletes the specified parsers. Cluster administrator privileges are required to call this API.

#### HTTP Request

DELETE /api/sonar/parsers

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/parsers?codes=test"

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| codes | O | String | Parser code list | Comma-separated list |

#### Success Response

{ "failures": {}}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "codes should be not null"}

Failed to delete parsers

HTTP status code 200

{ "failures": { "unknown": ["not-exist"] }}

* **failures** (Map): List of parsers that failed to delete. An array of parser identifiers as keys and reasons for failed deletions as values.
* not-exist: Parser is not found.
* referenced-by-logger-model: referenced by the logger model
* referenced-by-extractor-model: referenced by the extractor model

### Test Parser

#### HTTP Request

POST /api/sonar/parsers/:code/test

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d line="<36>[SNIPER-2000] [Attack\_Name=(0023)UDP Check Sum Error], [Time=2013/05/14 14:32:05], [Hacker=130.1.254.133], [Victim=130.1.213.10], [Protocol=udp/514], [Risk=Medium], [Handling=Alarm], [Information=], [SrcPort=514]" \ -X POST \ https://HOSTNAME/api/sonar/parsers/sniper/test

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| code | O | String | Parser code |  |
| line | O | String | Target test string |  |

#### Success Response

Below is the result of parsing the SNIPER IPS log as in the cURL example.

{ "rows": [ { "time": "2013-05-14 14:32:05+0900", "risk": "MEDIUM", "category": null, "host\_name": "SNIPER-2000", "src\_ip": "130.1.254.133", "src\_port": 514, "dst\_ip": "130.1.213.10" "dst\_port": 514, "protocol": "UDP", "hack\_code": "0023", "signature": "(0023)UDP Check Sum Error", "action": "DETECT", } ]}

* **rows** (Array): List of parsing result records. Field and value configuration depends on parser setting.

#### Error Responses

Parser is not found

{ "error\_code": "illegal-state", "error\_msg": "parser profile not found: unknown"}

Parsing failed

If the parsing fails, it returns the original data as is in the line field.

{ "rows": [ { "line": "Hello world," } ]}

### Get Log Schemas

Gets a list of log schemas that match the specified search keyword.

#### HTTP Request

GET /api/sonar/log-schemas

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/log-schemas

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load | If not specified, load all records |
| keywords | X | String | Keyword | Search available by code, name, description |

#### Success Response

Below is an example of searching by the keyword session.

{ "total\_count": 1, "schemas": [ { "code": "session", "name": "세션", "description": "방화벽 세션 및 네트워크 플로우", "created": "2022-09-01 00:31:13+0900" } ]}

* **total\_count** (32-bit integer): Total number of the log schemas that match the specified search keyword
* **schemas** (Array): Log schema list
* **code** (String): Code (Max. 50 characters). Identifier written to the \_schema field of the normalized log.
* **name** (String): Name (Max. 50 characters)
* **description** (String): Description (Max. 255 characters)
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### Get Log Schema

Retrieves data structure for a specified log schema.

#### HTTP Request

GET /api/sonar/log-schemas/:code

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/log-schemas/session

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| code | O | String | Log schema code |  |

#### Success Response

Below is an example of retrieving the session log schema.

{ "schema": { "code": "session", "name": "Session", "description": "Firewall traffic or flow log.", "created": "2022-09-01 00:31:13+0900", "fields": [ { "name": "\_time", "display\_name": "Time", "type": "DATE", "ordinal": 1 }, { "name": "src\_ip", "display\_name": "Source IP", "type": "IP", "ordinal": 2 }, { "name": "src\_port", "display\_name": "Source Port", "type": "PORT", "ordinal": 3 }, { "name": "dst\_ip", "display\_name": "Destination IP", "type": "IP", "ordinal": 4 }, { "name": "dst\_port", "display\_name": "Destination Port", "type": "PORT", "ordinal": 5 }, { "name": "protocol", "display\_name": "Protocol", "type": "STRING", "ordinal": 6 }, { "name": "app", "display\_name": "App", "type": "STRING", "ordinal": 7 }, { "name": "action", "display\_name": "Action", "type": "STRING", "ordinal": 8 }, { "name": "nat\_src\_ip", "display\_name": "NAT Source IP", "type": "IP", "ordinal": 9 }, { "name": "nat\_src\_port", "display\_name": "NAT Source Port", "type": "PORT", "ordinal": 10 }, { "name": "nat\_dst\_ip", "display\_name": "NAT Destination IP", "type": "IP", "ordinal": 11 }, { "name": "nat\_dst\_port", "display\_name": "NAT Destination Port", "type": "PORT", "ordinal": 12 }, { "name": "policy", "display\_name": "Policy", "type": "STRING", "ordinal": 13 }, { "name": "duration", "display\_name": "Duration", "type": "LONG", "ordinal": 14 }, { "name": "total\_bytes", "display\_name": "Bytes", "type": "STRING", "ordinal": 15 }, { "name": "total\_pkts", "display\_name": "Packets", "type": "STRING", "ordinal": 16 }, { "name": "sent\_pkts", "display\_name": "Sent Packets", "type": "LONG", "ordinal": 17 }, { "name": "rcvd\_pkts", "display\_name": "Received Packets", "type": "LONG", "ordinal": 18 }, { "name": "sent\_bytes", "display\_name": "Sent Bytes", "type": "LONG", "ordinal": 19 }, { "name": "rcvd\_bytes", "display\_name": "Received Bytes", "type": "LONG", "ordinal": 20 }, { "name": "src\_country", "display\_name": "Source Country", "type": "COUNTRY", "ordinal": 21 }, { "name": "dst\_country", "display\_name": "Destination Country", "type": "COUNTRY", "ordinal": 22 } ] }}

* **schema** (Map): Log schema definition
* **code** (String): Code
* **name** (String): Name
* **description** (String): Description
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **fields** (Array): List of normalized field definitions
* **name** (String): Field name
* **display\_name** (String): Display name
* **type** (String): Type. One of the following: DATE, STRING, IP, PORT, INT, LONG, DOUBLE, COUNTRY, MD5, SHA1, URL.
* **ordinal** (32-bit integer): Field display order

#### Error Responses

Log schema is not found

HTTP status code 200

{ "schema": null}

### Create Log Schema

Creates a new log schema.

#### HTTP Request

POST /api/sonar/log-schemas

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d code="ping" \ -d name="Ping" \ -d fields="[{""name"":""\_time"", ""type"":""DATE"", ""display\_name"":""Time"", ""ordinal"":1}, {""name"":""dst\_ip"", ""type"":""IP"", ""display\_name"":""Destination IP"", ""ordinal"":2}, {""name"":""rtt"", ""type"":""INT"", ""display\_name"":""Round trip time"", ""ordinal"":2}]" \ -X POST \ https://HOSTNAME/api/sonar/log-schemas

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| code | O | String | Log schema code | Minumum 1 to maximum 50 characters |
| name | O | String | Log schema name | Minumum 1 to maximum 50 characters |
| description | X | String | Log schema description | Maximum 255 characters |
| fields | X | String | Field definition list | JSON Array |

fieldsis JSON array string that contains the following properties:

* **type** (String): Field type
* One of the following: DATE, STRING, IP, PORT, INT, LONG, DOUBLE, COUNTRY, MD5, SHA1, URL.
* **name** (String): Field name (Maximum 50 characters)
* **display\_name** (String): Display name (Maximum 50 characters)
* **ordinal** (32-bit integer): Field order

#### Success Response

{}

#### Error Responses

No privilege to create a log schema

HTTP status code 500. A log schema is applied system-wide. To create a log schema, cluster administrator privileges are required.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

Required argument is missing

HTTP status code 400.

{ "error\_code": "null-argument", "error\_msg": "code should be not null"}

Invalid argument length

HTTP status code 400.

{ "error\_code": "invalid-argument", "error\_msg": "'code' must be less than or equal to 50 characters."}

Duplicated log schema ID

{ "error\_code": "illegal-state", "error\_msg": "duplicated log schema code: ping"}

### Update Log Schema

Updates an existing log schema.

#### HTTP Request

PUT /api/sonar/log-schemas/:code

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="Ping" \ -d fields="[{""name"":""\_time"", ""type"":""DATE"", ""display\_name"":""Time"", ""ordinal"":1}, {""name"":""src\_ip"", ""type"":""IP"", ""display\_name"":""SourceIP"", ""ordinal"":2}, {""name"":""dst\_ip"", ""type"":""IP"", ""display\_name"":""DestinationIP"", ""ordinal"":3},{""name"":""rtt"", ""type"":""INT"", ""display\_name"":""RoundTripTime"", ""ordinal"":4}]" \ -X PUT \ https://HOSTNAME/api/sonar/log-schemas/ping

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| code | O | String | Log schema code | Minimum 1 to maximum 50 characters |
| name | O | String | Log schema name | Minimum 1 to maximum 50 characters |
| description | X | String | Log schema description | Maximum 255 characters |
| fields | X | String | List of field definitions | JSON array |

fieldsis JSON array string that contains the following properties:

* **type** (String): Field type
* One of the following: DATE, STRING, IP, PORT, INT, LONG, DOUBLE, COUNTRY, MD5, SHA1, URL.
* **name** (String): Name (Max. 50 characters)
* **display\_name** (String): Display name (Max. 50 characters)
* **ordinal** (32-bit integer): Field order

#### Success Response

{}

#### Error Responses

No privilege to create a log schema

HTTP status code 500. Log schema is applied system wide. To create a log schema, cluster administrator privileges are required.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

Required argument is missing

HTTP status code 400.

{ "error\_code": "null-argument", "error\_msg": "code should be not null"}

Invalid argument length

HTTP status code 400.

{ "error\_code": "invalid-argument", "error\_msg": "'code' must be less than or equal to 50 characters."}

Log schema is not found

{ "error\_code": "illegal-state", "error\_msg": "log schema not found: test"}

### Remove Log Schema

Deletes specified log schemas.

#### HTTP Request

DELETE /api/sonar/table-schemas

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/table-schemas?codes=ping"

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| codes | O | String | Log schema code list | Comma-separated list |

#### Success Response

{ "failures": []}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "codes should be not null"}

Failed to delete log schema

HTTP status code 200

{ "failures": [ { "id": "session", "reason": "referenced-by-object" }, { "id": "ping2", "reason": "table-schema-not-found" } ]}

* **failures** (Array): List of log schemas that failed to delete
* **id** (String): Log schema code
* **reason** (String): Cause of failure
* Log schema is not found. (log-schema-not-found)
* Log schema is referenced by extract model or other objects. (referenced-by-object)

## Logger Factory API

### Get Logger Factories

Gets the list of the logger factories on a specified server or across the entire cluster.

#### HTTP Request

GET /api/sonar/logger-factories

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/logger-factories

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| node\_pair\_guid | X | String | Node pair GUID | 36 characters. GUID of the node pair from which to get the list of logger factories. |

#### Success Response

A successful response returns the name and description of the logger factories according to locale language of the account associated with the API key. The results are output in ascending order by display name (display\_name).

{ "logger\_factories": [ { "name": "cepevent", "display\_name": "CEP 이벤트", "description": "CEP 컨텍스트 이벤트를 수집합니다." }, { "name": "tap-dns", "display\_name": "DNS 스니퍼", "description": "네트워크를 미러링하여 DNS 패킷을 기록합니다." }, { "name": "ftp-dirwatch", "display\_name": "FTP 디렉터리 와처", "description": "지정된 FTP 서버 디렉터리에서 파일이름 패턴과 일치하는 모든 텍스트 로그 파일을 수집합니다." }, { "name": "ftp-rotation", "display\_name": "FTP 로테이션 로그 파일", "description": "FTP를 통해 일정 주기마다 다른 경로에 백업 후 삭제하고 다시 쓰는 로그 파일을 수집합니다." }, { "name": "ftp-daily-rolling-dirwatch", "display\_name": "FTP 일자별 디렉터리", "description": "FTP를 이용하여 일자별로 생성되는 디렉터리를 순회하면서 파일 이름 패턴과 일치하는 모든 텍스트 로그 파일을 수집합니다." }, { "name": "gzip-dirwatch", "display\_name": "GZIP 디렉터리 와처", "description": "지정된 디렉터리에서 파일이름 패턴과 일치하는 모든 gzip 파일을 수집합니다." }, { "name": "http-post", "display\_name": "HTTP POST", "description": "HTTP POST를 통해 로그를 수신합니다." }, { "name": "http-monitor", "display\_name": "HTTP 모니터", "description": "웹 서비스 응답 코드와 통계 정보를 수집합니다." }, { "name": "tap-http", "display\_name": "HTTP 스니퍼", "description": "네트워크를 미러링하여 HTTP 패킷을 기록합니다." }, { "name": "jdbc", "display\_name": "JDBC 수집기", "description": "JDBC를 통해 데이터베이스에서 데이터를 수집합니다." }, { "name": "netflow", "display\_name": "NetFlow", "description": "UDP를 통해 넷플로우 v5와 v9 패킷을 수신합니다." }, { "name": "pcap-dirwatch", "display\_name": "PCAP 디렉터리 와처", "description": "디렉터리에서 PCAP 파일을 수집합니다." }, { "name": "pcap", "display\_name": "PCAP 패킷", "description": "PCAP 스트림을 통해 패킷를 수집합니다." }, { "name": "rss", "display\_name": "RSS 수집기", "description": "RSS 통해 로그를 수신합니다." }, { "name": "sftp-wtmp", "display\_name": "SFTP WTMP 파일", "description": "SFTP 서버를 통해 wtmp 로그 파일을 수집합니다." }, { "name": "sftp-dirwatch", "display\_name": "SFTP 디렉터리 와처", "description": "원격 SFTP 서버에 접속하여 텍스트 로그 파일을 수집합니다." }, { "name": "sftp-rotation", "display\_name": "SFTP 로테이션 로그 파일", "description": "SFTP를 통해 일정 주기마다 다른 경로에 백업 후 삭제하고 다시 쓰는 로그 파일을 수집합니다." }, { "name": "sftp-multi-rotation", "display\_name": "SFTP 멀티 로테이션 로그 파일", "description": "원격 SFTP 서버에 접속하여 일정 주기마다 다른 경로에 백업 후 삭제하고 다시 쓰는 로그 파일들을 수집합니다." }, { "name": "sftp-daily-rolling-dirwatch", "display\_name": "SFTP 일자별 디렉터리", "description": "SFTP를 이용하여 일자별로 생성되는 디렉터리를 순회하면서 파일 이름 패턴과 일치하는 모든 텍스트 로그 파일을 수집합니다." }, { "name": "snmpget", "display\_name": "SNMP GET", "description": "SNMP GET 호출을 이용하여 OID 값을 수집합니다." }, { "name": "snmpmon", "display\_name": "SNMP 인터페이스 통계", "description": "SNMP 쿼리를 통해 인터페이스별 트래픽 통계를 수집합니다." }, { "name": "snmptrap", "display\_name": "SNMP 트랩 수신기", "description": "UDP로 SNMP 트랩 패킷을 수신합니다." }, { "name": "snmpv3get", "display\_name": "SNMPv3 GET", "description": "SNMPv3 GET 호출을 이용하여 OID 값을 수집합니다." }, { "name": "snmpmonv3", "display\_name": "SNMPv3 인터페이스 통계", "description": "SNMPv3 쿼리를 통해 인터페이스별 트래픽 통계를 수집합니다." }, { "name": "ssh-exec", "display\_name": "SSH 실행", "description": "SSH 쉘의 표준 출력을 로그로 수집합니다." }, { "name": "port-check", "display\_name": "TCP 포트 상태 수집기", "description": "TCP 포트의 개방 여부를 확인합니다." }, { "name": "wtmp", "display\_name": "WTMP", "description": "터미널 로그인, 로그아웃 기록을 수집합니다." }, { "name": "sflow", "display\_name": "sFlow", "description": "UDP를 통해 에스플로우 v5 패킷을 수신합니다." }, { "name": "dirwatch", "display\_name": "디렉터리 와처", "description": "지정된 디렉터리에서 파일이름 패턴과 일치하는 모든 텍스트 로그 파일을 수집합니다." }, { "name": "disk-usage", "display\_name": "디스크 사용량", "description": "디스크 사용량을 주기적으로 모니터링합니다." }, { "name": "rotation", "display\_name": "로테이션 로그 파일", "description": "일정 주기마다 다른 경로에 백업 후 삭제하고 다시 쓰는 로그 파일을 수집합니다." }, { "name": "linux-account-watch", "display\_name": "리눅스 계정 이벤트 탐지", "description": "계정이 추가/삭제될 때마다 로그를 발생합니다." }, { "name": "gzip-recursive-dirwatch", "display\_name": "리커시브 GZIP 디렉터리 와처", "description": "지정된 디렉터리에서 파일이름 패턴과 일치하는 모든 텍스트 GZIP 로그 파일을 수집합니다." }, { "name": "recursive-dirwatch", "display\_name": "리커시브 디렉터리 와처", "description": "지정된 디렉터리에서 파일이름 패턴과 일치하는 모든 텍스트 로그 파일을 수집합니다." }, { "name": "multi-rotation", "display\_name": "멀티 로테이션 로그 파일", "description": "일정 주기마다 다른 경로에 백업 후 삭제하고 다시 쓰는 로그 파일들을 수집합니다." }, { "name": "config-watch", "display\_name": "설정 파일 변경 탐지", "description": "설정 파일이 변경될 때마다 로그를 발생합니다." }, { "name": "sentry-perf", "display\_name": "센트리 성능 로그", "description": "로그프레소 센트리 성능 로그를 일괄 수집합니다." }, { "name": "stream", "display\_name": "스트림 쿼리 출력", "description": "스트림 쿼리의 출력을 수집합니다." }, { "name": "syslog", "display\_name": "시스로그 수집기", "description": "시스로그(TCP/UDP) 포트를 통해 시스로그를 수신합니다." }, { "name": "exec", "display\_name": "외부프로그램", "description": "외부 프로그램의 표준 출력을 로그로 수집합니다." }, { "name": "daily-dirwatch", "display\_name": "일자별 디렉터리", "description": "일자별로 생성되는 디렉터리를 순회하면서 파일 이름 패턴과 일치하는 모든 텍스트 로그 파일을 수집합니다." } ]}

* **logger\_factories** (Array): List of logger factories
* **name** (String): Logger factory identifier
* **display\_name** (String): Logger factory display name
* **description** (String): Logger factory description

### Get Logger Factory

Retrieves information of a specified logger factory.

#### HTTP Request

GET /api/sonar/logger-factories/:node\_pair\_guid/:namespace/:name

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/logger-factories/27102ae5-3698-44d4-aad5-4f2def80f275/local/syslog

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| node\_pair\_guid | O | String | Node pair GUID | 36 characters |
| namespace | O | String | Namespace | local or sentry identifier |
| name | O | String | Identifier | E.g. syslog, dirwatch |

#### Success Response

{ "logger\_factory": { "full\_name": "local\\syslog", "display\_group": "시스로그", "group": "Syslog", "display\_name": "시스로그 수집기", "namespace": "local", "name": "syslog", "description": "시스로그(TCP/UDP) 포트를 통해 시스로그를 수신합니다." }}

* **logger\_factory** (Map): Logger factory
* **full\_name** (String): Name in namespace\identifier format
* **name** (String): Identifier
* **display\_group** (String): Display name in locale language
* **group** (String): Group identifier
* **display\_name** (String): Display name in locale language
* **namespace** (String): Namespace. local or sentry identifier
* **description** (String): Description

### Get Logger Factory Options

Retrieves the configuration options of a specified logger factory.

#### HTTP Request

GET /api/sonar/logger-factories/:node\_pair\_guid/:namespace/:name/options

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/logger-factories/27102ae5-3698-44d4-aad5-4f2def80f275/local/syslog/options

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| node\_pair\_guid | O | String | Node pair GUID | 36 characters |
| namespace | O | String | Namespace | local or sentry identifier |
| name | O | String | Identifier | E.g. syslog, dirwatch |

#### Success Response

{ "options": [ { "type": "string", "subtype": "ip-range", "name": "remote\_ip", "required": false, "display\_name": "원격지 IP", "description": "원격지 IP 주소 또는 범위, 예를 들면 IP 또는 IP1-IP2 또는 IP/CIDR", "default\_value": null }, { "type": "string", "subtype": "port", "name": "dst\_port", "required": false, "display\_name": "포트", "description": "수신 포트 필터(설정하지 않은 경우 모든 포트에 대하여 수신합니다.)", "default\_value": null }, { "type": "string", "subtype": null, "name": "facility", "required": false, "display\_name": "시스로그 설비 목록", "description": "쉼표(`,`)로 구분된 시스로그 설비 번호", "default\_value": null }, { "type": "string", "subtype": "regex", "name": "date\_pattern", "required": false, "display\_name": "날짜 정규표현식", "description": "날짜 및 시각을 추출하는데 사용할 정규표현식", "default\_value": null }, { "type": "string", "subtype": "date-format", "name": "date\_format", "required": false, "display\_name": "날짜 포맷", "description": "날짜 및 시각 문자열을 파싱하는데 사용할 포맷. 예) yyyy-MM-dd HH:mm:ss", "default\_value": null }, { "type": "string", "subtype": "date-locale", "name": "date\_locale", "required": false, "display\_name": "날짜 로케일", "description": "날짜 로케일, 예를 들면 ko", "default\_value": null }, { "type": "string", "subtype": "timezone", "name": "timezone", "required": false, "display\_name": "시간대", "description": "시간대, 예를 들면 KST 또는 Asia/Seoul", "default\_value": null }, { "type": "string", "subtype": "regex", "name": "regex", "required": false, "display\_name": "정규식 필터", "description": "추출할 데이터를 선별할 정규식 패턴", "default\_value": null } ]}

* **options** (Array): Options list
* **type** (String): Value type. Either string, integer, or boolean.
* **subtype** (String): UI rendering hint. Either date-format, date-locale, ip-range, port, regex, or timezone.
* **name** (String): Variable name
* **required** (Boolean): Whether the option is required
* **display\_name** (String): Display name
* **description** (String): Description
* **default\_value** (String): Default setting in a logger configuration

### Get Logger Models

Gets the list of logger models.

#### HTTP Request

GET /api/sonar/logger-models

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/logger-models?offset=0&limit=10

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records |  |
| keywords | X | String | Search available by logger model name name |  |

#### Success Response

{ "total\_count": 2, "logger\_models": [ { "guid": "cd09ae6f-fbc3-11ed-9320-02d178f999a6", "name": "WTMP", "description": null, "logger\_factory\_name": "wtmp", "logger\_factory\_display\_name": "WTMP", "parser\_code": null, "parser\_name": null, "app\_code": null, "app\_built\_in": null, "rule\_count": 1, "created": "2023-10-01 09:18:27+0900", "updated": "2023-10-01 09:18:27+0900" }, { "guid": "cd09b2b7-fbc3-11ed-9320-02d178f999a6", "name": "윈도우 XML 이벤트 로그", "description": null, "logger\_factory\_name": "windows-evtx", "logger\_factory\_display\_name": null, "parser\_code": null, "parser\_name": null, "app\_code": null, "app\_built\_in": null, "rule\_count": 1, "created": "2023-10-01 09:18:27+0900", "updated": "2023-10-01 09:18:27+0900" } ]}

* **total\_count** (32-bit integer): Total number of logger models that match the search keyword
* **logger\_models** (Array): Logger model list
* **guid** (String): Logger model GUID
* **name** (String): Logger model name
* **description** (String): Logger model description
* **logger\_factory\_name** (String): Logger factory identifier
* **logger\_factory\_display\_name** (String): Display name of the logger factory
* **parser\_code** (String): Parser identifier
* **parser\_name** (String): Parser name
* **app\_code** (String): App code as identifier
* **app\_built\_in** (Boolean): Whether the logger model is built in the app
* **rule\_count** (32-bit integer): Total number of normalization rules
* **created** (String): Creation date and time (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Last modification date and time (yyyy-MM-dd HH:mm:ssZ)

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### Get Logger Model

Retrieves information of a specified logger model.

#### HTTP Request

GET /api/sonar/logger-models/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/logger-models/cd09ae6f-fbc3-11ed-9320-02d178f999a6

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Logger model identifier | 36-characters GUID |

#### Success Response

{ "logger\_model": { "guid": "cd09ae6f-fbc3-11ed-9320-02d178f999a6", "name": "WTMP", "description": null, "logger\_factory\_name": "wtmp", "logger\_factory\_display\_name": "WTMP", "parser\_code": null, "parser\_name": null, "app\_code": null, "app\_built\_in": null, "rule\_count": 1, "rules": [ { "guid": "cd0cdd74-fbc3-11ed-9320-02d178f999a6", "name": "WTMP - 인증", "log\_schema\_code": "auth", "log\_schema\_name": "인증", "parser\_code": null, "parser\_name": null, "stream\_query": "eval action = case(type == \"UserProcess\", \"LOGIN\", type == \"DeadProcess\", \"LOGOUT\"), src\_ip = ip(host), user = if(len(user) == 0, null, user)", "stream\_interval": 60, "app\_code": null, "app\_built\_in": null } ], "created": "2023-10-01 09:18:27+0900", "updated": "2023-10-01 09:18:27+0900" }}

* **logger\_model** (Map): Logger model
* **guid** (String): Logger model identifier
* **name** (String): Logger model name
* **description** (String): Logger model description
* **logger\_factory\_name** (String): Logger factory identifier
* **logger\_factory\_display\_name** (String): Logger factory display name
* **parser\_code** (String): Parser identifier
* **parser\_name** (String): Parser name
* **app\_code** (String): App code as identifier
* **app\_built\_in** (Boolean): Whether the logger model is built in the app
* **rule\_count** (32-bit integer): Total number of normalization rules
* **rules** (Array): Normalization rule list
* **guid** (String): Normalization rule identifier
* **name** (String): Normalization rule name
* **log\_schema\_code** (String): Log schema identifier
* **log\_schema\_name** (String): Log schema name
* **parser\_code** (String): Parser identifier
* **parser\_name** (String): Parser name
* **stream\_query** (String): Stream query
* **stream\_interval** (32-bit integer): Stream query refresh interval
* **app\_code** (String): App code as identifier
* **app\_built\_in** (Boolean): Whether the logger model is built in the app
* **created** (String): Creation date and time (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Last modification date and time (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Logger model is not found

HTTP status code 200

{ "logger\_model": null}

### Create Logger Model

Creates a new logger model. Administrator privileges are required to call this API.

#### HTTP Request

POST /api/sonar/logger-models

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="NGINX" \ -d logger\_factory\_name="dirwatch" \ -d 'rules=[{"name": "Web log", "log\_schema\_code": "web", "stream\_query": "rex field=line \"(?<src\_ip>\\S+) \\S+ \\S+ \\[(?<event\_time>\\S+ \\S+)\\] \\\"\\S+ \\S+ \\S+\\\" (?<status>\\d+) (?<sc\_bytes>\\d+) \\S+ \\\"(?<user\_agent>[^\\\"]+)\" | eval event\_time = date(event\_time, \"dd/MMM/yyyy:HH:mm:ss Z\"), src\_ip = ip(src\_ip), sc\_bytes = long(sc\_bytes)", "stream\_interval": 0}]' \ -X POST https://HOSTNAME/api/sonar/logger-models

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | X | String | Logger model identifier | 36-characters GUID. If not specified, randomly generated. |
| name | O | String | Logger model name | Minimum 1 to maximum 50 characters. |
| description | X | String | Logger model description | Maximum 2,000 characters |
| logger\_factory\_name | O | String | Logger factory identifier |  |
| parser\_code | X | String | Parser identifier |  |
| rules | X | Object array | List of normalization rules | See "rules attributes" below. |

`rules` attributes

* **guid** (String): Normalization rule identifier. If not specified, randomly generated.
* **name** (String): Normalization rule name
* **log\_schema\_code** (String): Log schema identifier
* **stream\_query** (String): Stream query string
* **stream\_interval** (32-bit integer): Stream query refresh interval

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

Parser is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "parser not found: nginx"}

Logger model is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "logger factory not found: unknown"}

Duplicated logger model name

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "duplicated logger model name: NGINX"}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Update Logger model

Updates a specified logger model. Administrator privileges are required to call this API.

#### HTTP Request

PUT /api/sonar/logger-models/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="NGINX" \ -d description="Demo" \ -d 'rules=[{"name": "Web log", "log\_schema\_code": "web", "stream\_query": "rex field=line \"(?<src\_ip>\\S+) \\S+ \\S+ \\[(?<event\_time>\\S+ \\S+)\\] \\\"\\S+ \\S+ \\S+\\\" (?<status>\\d+) (?<sc\_bytes>\\d+) \\S+ \\\"(?<user\_agent>[^\\\"]+)\" | eval event\_time = date(event\_time, \"dd/MMM/yyyy:HH:mm:ss Z\"), src\_ip = ip(src\_ip), sc\_bytes = long(sc\_bytes)", "stream\_interval": 0}]' \ -X PUT https://HOSTNAME/api/sonar/logger-models

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | X | String | Logger model identifier | 36-characters GUID. If not specified, randomly generated. |
| name | O | String | Logger model name | Minimum 1 to maximum 50 characters. |
| description | X | String | Logger model description | Maximum 2,000 characters |
| parser\_code | X | String | Parser identifier |  |
| rules | X | Object array | List of normalization rules | See rules attributes below |

`rules`` attributes

* (String) guid: Normalization rule identifier. If not specified, randomly generated.
* (String) name: Normalization rule name
* (String) log\_schema\_code: Log schema identifier
* (String) stream\_query: Stream query string
* (32-bit integer) stream\_interval: Stream query refresh interval

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

Parser is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "parser not found: nginx"}

Duplicated logger model name

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "duplicated logger model name: NGINX"}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Remove Logger Models

Removes specified logger models. Administrator privileges are required to call this API.

#### HTTP Request

DELETE /api/sonar/logger-models

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids="54157629-74f7-4d80-be5a-8cb8f0c71087" \ -X DELETE https://HOSTNAME/api/sonar/logger-models

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guids | O | List of strings | Logger model GUID list | Comma-separated GUID list |

#### Success Response

{ "failures": []}

#### Error Responses

Logger model is not found

HTTP status code 200

{ "failures": [ { "id": "c1dfe306-abba-4ed8-862b-0e98e2effcb6", "reason": "logger-model-not-found" } ]}

Logger model is referenced by other loggers

HTTP status code 200

{ "failures": [ { "id": "cd09ae6f-fbc3-11ed-9320-02d178f999a6", "name": "WTMP", "reason": "referenced-by-loggers" } ]}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Get Logger Groups

Gets the list of logger groups.

#### HTTP Request

GET /api/sonar/logger-groups

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/logger-groups?offset=0&limit=10

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load | Default: unlimited |

#### Success Response

{ "total\_count": 1, "logger\_groups": [ { "guid": "0565a218-a78d-43ff-89b6-a9899adcf8c5", "name": "Firewall", "description": null, "parent\_guid": null, "created": "2023-10-01 22:20:44+0900", "updated": "2023-10-01 22:20:44+0900" } ]}

* **total\_count** (32-bit integer): Total number of logger groups that match the search keyword
* **logger\_groups** (Array): Logger group list
* **guid** (String): Logger group GUID
* **name** (String): Logger group name
* **description** (String): Logger group description
* **parent\_guid** (String): Parent logger group identifier
* **created** (String): Creation date and time (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Last modification date and time (yyyy-MM-dd HH:mm:ssZ)

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is not negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### Get Logger Group

Retrieves information of a specified logger group.

#### HTTP Request

GET /api/sonar/logger-groups/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/logger-groups/0565a218-a78d-43ff-89b6-a9899adcf8c5

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Logger group identifier | 36-characters GUID |

#### Success Response

{ "logger\_group": { "guid": "0565a218-a78d-43ff-89b6-a9899adcf8c5", "name": "Firewall", "description": null, "parent\_guid": null, "created": "2023-10-01 22:20:44+0900", "updated": "2023-10-01 22:20:44+0900" }}

* **logger\_group** (Map): Logger group
* **guid** (String): Logger group identifier
* **name** (String): Logger group name
* **description** (String): Logger group description
* **parent\_guid** (String): Parent logger group identifier
* **created** (String): Creation date and time (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Last modification date and time (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Logger group is not found

HTTP status code 200

{ "logger\_group": null}

### Create Logger Group

Creates a new logger group. Administrator privileges are required to call this API.

#### HTTP Request

POST /api/sonar/logger-groups

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="Firewall" \ -X POST https://HOSTNAME/api/sonar/logger-groups

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | X | String | Logger group identifier | 36-characters GUID. If not specified, randomly generated. |
| name | O | String | Logger group name | Minimum 1 to maximum 50 characters. |
| description | X | String | Logger group description | Maximum 2,000 characters |
| parent\_guid | X | String | Parent logger group identifier | 36-characters GUID |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Update Logger Group

Updates a specified logger group. Administrator privileges are required to call this API.

#### HTTP Request

PUT /api/sonar/logger-groups/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="Firewall" \ -d parent\_guid="54157629-74f7-4d80-be5a-8cb8f0c71087" \ -X PUT https://HOSTNAME/api/sonar/logger-groups/0565a218-a78d-43ff-89b6-a9899adcf8c5

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Logger group identifier | 36-characters GUID |
| name | O | String | Logger group name | Minimum 1 to maximum 50 characters. |
| description | X | String | Logger group description | Maximum 2,000 characters |
| parent\_guid | X | String | Parent logger group identifier | 36-characters GUID |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Remove Logger Groups

Revmoves specified logger groups. Administrator privileges are required to call this API.

#### HTTP Request

DELETE /api/sonar/logger-groups

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids="54157629-74f7-4d80-be5a-8cb8f0c71087" \ -X DELETE https://HOSTNAME/api/sonar/logger-groups

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guids | O | List of strings | Logger group GUID list | Comma-separated GUID list |

#### Success Response

{ "failures": []}

#### Error Responses

Logger group is not found

HTTP status code 200

{ "failures": [ { "id": "c1dfe306-abba-4ed8-862b-0e98e2effcb6", "reason": "logger-group-not-found" } ]}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Get Loggers

Gets the list of the loggers

#### HTTP Request

GET /api/sonar/loggers

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/loggers?offset=0&limit=10

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records |  |
| keywords | X | String | Keyword | Search available by name |
| schema\_code | X | String | Log schema identifier | Filter criteria for the logger list in real-time detection scenario builder |

#### Success Response

{ "total\_count": 1, "loggers": [ { "id": 1, "guid": "b90ea540-4f47-4bcf-b708-af610a649c50", "name": "WTMP", "description": "", "table\_name": "WTMP", "interval": 5000, "cron\_schedule": null, "enabled": true, "status": "running", "failure": null, "is\_passive": false, "model\_guid": "cd09ae6f-fbc3-11ed-9320-02d178f999a6", "model\_name": "WTMP", "group\_guid": null, "group\_name": null, "node\_pair\_guid": "27102ae5-3698-44d4-aad5-4f2def80f275", "node\_pair\_name": "control", "sentry\_guid": null, "asset\_guid": null, "asset\_ip": null, "hostname": null, "log\_count": 892, "log\_volume": 97531, "drop\_count": 0, "drop\_volume": 0, "configs": { "path": "/var/log/wtmp", "server": null, "regex\_filter\_target\_field": null, "regex\_filter\_pattern": null, "regex\_filter\_negate": "false", "dst\_ip": null }, "created": "2023-10-01 23:59:22+0900", "updated": "2023-10-01 23:59:39+0900" } ]}

* **total\_count** (32-bit integer): Total number of loggers that match the search keyword
* **loggers** (Array): Logger list
* **id** (32-bit integer): Logger ID
* **guid** (String): Logger GUID
* **name** (String): Logger name
* **description** (String): Logger description
* **table\_name** (String): Name of the logger table on which the collected logs are stored
* **interval** (32-bit integer): Logger interval (Unit: milliseconds)
* **cron\_schedule** (String): Logger schedule in CRON schedule expression. E.g. 0 4 \* \* \* indicates to execute a task at 4:00 AM daily.
* **enabled** (Boolean): Whether the logger is enabled
* **status** (String): Running status. Either running or stopped (even if a logger is enabled, it may stop due to an error.)
* **failure** (String): Last failure reason. E.g. an SFTP logger may encounter an Auth fail error.
* **is\_passive** (Boolean): Whether the logger runs regardless of interval or schedule settings; a passive logger.
* **model\_guid** (String): Logger model identifier
* **model\_name** (String): Logger model name
* **site\_guid** (String): Site GUID as identifier
* **site\_name** (String): Site name
* **node\_pair\_guid** (String): Node pair identifier
* **node\_pair\_name** (String): Node pair name
* **sentry\_guid** (String): Sentry identifier
* **asset\_guid** (String): Asset IP address identifier
* **asset\_ip** (String): Asset IP address
* **hostname** (String): Asset IP hostname
* **log\_count** (64-bit integer): Total number of the collected logs. Excluding the logs filtered and dropped by a regular expression filter.
* **log\_volume** (64-bit integer): Total volume (in bytes) of the collected logs. Excluding the logs filtered and dropped by a regular expression filter.
* **drop\_count** (64-bit integer): Number of the logs filtered and dropped by a regular expression filter.
* **drop\_volume** (64-bit integer): Volume (in bytes) of the logs filtered and dropped by a regular expression filter.
* **configs** (Map): Logger configuration key/value pairs. Settings vary depending on the logger model or logger factory.
* **created** (String): Creation date and time (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Last modification date and time (yyyy-MM-dd HH:mm:ssZ)

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### Get Logger

Retrieves information of a specified logger.

#### HTTP Request

GET /api/sonar/loggers/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/loggers/b90ea540-4f47-4bcf-b708-af610a649c50

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Logger identifier | 36-characters GUID |

#### Success Response

{ "logger": { "id": 1, "guid": "b90ea540-4f47-4bcf-b708-af610a649c50", "name": "WTMP", "description": "", "table\_name": "WTMP", "interval": 5000, "cron\_schedule": null, "enabled": true, "status": "running", "failure": null, "is\_passive": false, "model\_guid": "cd09ae6f-fbc3-11ed-9320-02d178f999a6", "model\_name": "WTMP", "group\_guid": null, "group\_name": null, "node\_pair\_guid": "27102ae5-3698-44d4-aad5-4f2def80f275", "node\_pair\_name": "control", "sentry\_guid": null, "asset\_guid": null, "asset\_ip": null, "hostname": null, "log\_count": 892, "log\_volume": 97531, "drop\_count": 0, "drop\_volume": 0, "configs": { "path": "/var/log/wtmp", "server": null, "regex\_filter\_target\_field": null, "regex\_filter\_pattern": null, "regex\_filter\_negate": "false", "dst\_ip": null }, "created": "2023-10-01 23:59:22+0900", "updated": "2023-10-01 23:59:39+0900" }}

* **logger** (Map): Logger
* **id** (32-bit integer): Logger ID
* **guid** (String): Logger GUID
* **name** (String): Logger name
* **description** (String): Logger description
* **table\_name** (String): Name of the logger table on which the collected logs are stored
* **interval** (32-bit integer): Logger interval (Unit: milliseconds)
* **cron\_schedule** (String): Logger schedule in CRON schedule expression. E.g. 0 4 \* \* \* indicates to execute a task at 4:00 AM daily.
* **enabled** (Boolean): Whether the logger is enabled
* **status** (String): Running status. Either running or stopped (even if a logger is enabled, it may stop due to an error.)
* **failure** (String): Last failure reason. E.g. an SFTP logger may encounter an Auth fail error.
* **is\_passive** (Boolean): Whether the logger runs regardless of interval or schedule settings; a passive logger.
* **model\_guid** (String): Logger model GUID
* **model\_name** (String): Logger model name
* **site\_guid** (String): Site GUID
* **site\_name** (String): Site name
* **node\_pair\_guid** (String): Node pair GUID
* **node\_pair\_name** (String): Node pair name
* **sentry\_guid** (String): Sentry GUID
* **asset\_guid** (String): Asset IP address GUID
* **asset\_ip** (String): Asset IP address
* **hostname** (String): Asset IP hostname
* **log\_count** (64-bit integer): Total number of the collected logs. Excluding the logs filtered and dropped by a regular expression filter.
* **log\_volume** (64-bit integer): Total volume (in bytes) of the collected logs. Excluding the logs filtered and dropped by a regular expression filter.
* **drop\_count** (64-bit integer): Number of the logs filtered and dropped by a regular expression filter.
* **drop\_volume** (64-bit integer): Volume (in bytes) of the logs filtered and dropped by a regular expression filter.
* **configs** (Map): Logger configuration key/value pairs. Settings vary depending on the logger model or logger factory.
* **created** (String): Creation date and time (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Last modification date and time (yyyy-MM-dd HH:mm:ssZ)

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### Create Logger

Creates a new logger. Administrator privileges are required to call this API.

#### HTTP Request

POST /api/sonar/loggers

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d model\_guid="cd09ae6f-fbc3-11ed-9320-02d178f999a6" \ -d name="WTMP" \ -d node\_pair\_guid="27102ae5-3698-44d4-aad5-4f2def80f275" \ -d table\_name="WTMP" \ -d interval=5000 \ -d 'configs={"path": "/var/log/wtmp"}' \ -X POST https://HOSTNAME/api/sonar/loggers

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | X | String | Logger identifier | 36-characters GUID. If not specified, randomly generated. |
| model\_guid | O | String | Logger model identifier | 36-characters GUID |
| name | O | String | Logger name | Minimum 1 to maximum 50 characters. |
| description | X | String | Logger description | Maximum 2,000 characters |
| node\_pair\_guid | O | String | Node pair identifier | 36 characters |
| table\_name | O | String | Table name |  |
| sentry\_guid | X | String | Sentry identifier |  |
| interval | X | 32-bit integer | Logger interval | Minimum 1000 (Unit: milliseconds) |
| cron\_schedule | X | String | Logger schedule | CRON schedule expression |
| asset\_guid | X | String | Asset identifier | Asset IP address |
| configs | X | Key/value string | Configuration details | See [Get Logger Factory Options](https://docs.logpresso.com/en/sonar/4.0/api/get-logger-factory-options). |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "asset\_guid should be guid type."}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

CRON schedule expression is not valid

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "wrong cron expression format: \* \* \* \*"}

Logger model is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "logger model not found: bd09ae6f-fbc3-11ed-9320-02d178f999a6"}

Node pair is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "node pair not found: 37102ae5-3698-44d4-aad5-4f2def80f275"}

Sentry is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "sentry not found: test"}

Asset is not found

{ "error\_code": "illegal-state", "error\_msg": "asset not found: cd09ae6f-fbc3-11ed-9320-02d178f999a6"}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Update Logger

Updates a specified logger. Administrator privileges are required to call this API.

#### HTTP Request

PUT /api/sonar/loggers/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="WTMP" \ -d description="demo" \ -d interval=10000 \ -d 'configs={"path": "/var/log/wtmp"}' \ -X PUT https://HOSTNAME/api/sonar/loggers/b90ea540-4f47-4bcf-b708-af610a649c50

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Logger GUID | 36-characters GUID |
| name | O | String | Logger name | Minimum 1 to maximum 50 characters. |
| description | X | String | Logger description | Maximum 2,000 characters |
| interval | X | 32-bit integer | Logger interval | Minimum 1000 (Unit: milliseconds) |
| cron\_schedule | X | String | Logger schedule 주기 |  |
| asset\_guid | X | String | Asset identifier | Asset IP address |
| configs | X | Key/Value string | Configuration details | See [Get Logger Factory Options](https://docs.logpresso.com/en/sonar/4.0/api/get-logger-factory-options). |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "asset\_guid should be guid type."}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

CRON schedule expression is not valid

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "wrong cron expression format: \* \* \* \*"}

Asset is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "asset not found: cd09ae6f-fbc3-11ed-9320-02d178f999a6"}

Logger is not found

{ "error\_code": "illegal-state", "error\_msg": "logger not found: c90ea540-4f47-4bcf-b708-af610a649c50"}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Remove Logger

Removes a specified logger. Administrator privileges are required to call this API.

#### HTTP Request

DELETE /api/sonar/loggers/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE https://HOSTNAME/api/sonar/loggers/b90ea540-4f47-4bcf-b708-af610a649c50

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Logger identifier | 36-characters GUID |
| drop\_table | X | Boolean | Whether to drop table as well | Default: false |

#### Success Response

{}

Logger identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Remove Loggers

Removes specified loggers. Administrator privileges are required to call this API.

#### HTTP Request

DELETE /api/sonar/loggers

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids="54157629-74f7-4d80-be5a-8cb8f0c71087" \ -X DELETE https://HOSTNAME/api/sonar/loggers

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guids | O | List of strings | Logger GUID list | Comma-separated GUID list |
| drop\_table | X | Boolean | Whether to drop table as well | Default: false |

#### Success Response

{ "failures": []}

#### Error Responses

Table is referenced by other loggers

HTTP status code 200

{ "failures": [ { "id": "3a2e6570-3a5e-4b2f-982f-037eff266139", "name": "WTMP2", "reason": "table is referenced by other loggers: WTMP" } ]}

Logger identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Enable Logger

Enables a specified logger. Administrator privileges are required to call this API.

#### HTTP Request

POST /api/sonar/loggers/:guid/enable

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST https://HOSTNAME/api/sonar/loggers/b90ea540-4f47-4bcf-b708-af610a649c50/enable

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Logger identifier | 36-characters GUID |

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Logger is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "logger not found: 05efb651-9644-4518-950f-dbd648c973a7"}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Disable Logger

Disables a specified logger. Administrator privileges are required to call this API.

#### HTTP Request

POST /api/sonar/loggers/:guid/disable

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST https://HOSTNAME/api/sonar/loggers/b90ea540-4f47-4bcf-b708-af610a649c50/disable

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Logger identifier | 36-characters GUID |

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Logger is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "logger not found: 05efb651-9644-4518-950f-dbd648c973a7"}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Reset Loggers

Resets specified loggers. Once a logger is reset, it restarts logging from scratch. Administrator privileges are required to call this API.

#### HTTP Request

DELETE /api/sonar/loggers/states

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE https://HOSTNAME/api/sonar/loggers/states

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guids | O | List of strings | Logger GUID list | Comma-separated GUID list |

#### Error Responses

#### Success Response

{ "failures": []}

#### Error Responses

Logger is not found

HTTP status code 200

{ "failures": [ { "id": "c1dfe306-abba-4ed8-862b-0e98e2effcb6", "reason": "logger-not-found" } ]}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## Address Group API

### Get Address Groups

Gets a list of available address groups.

#### HTTP Request

GET /api/sonar/address-groups

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ "https://HOSTNAME/api/sonar/address-groups?offset=0&limit=20"

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load | Default: 2147483647 |
| keywords | X | String | Keywords | Search available by name, description |

#### Success Response

{ "total\_count": 1, "address\_groups": [ { "guid": "4dc14f3d-ebf8-4032-8a7a-ef9ec6cd3dd2", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "로그프레소", "name": "방화벽 차단 IP", "description": "차단 연동용 IP 블랙리스트", "count": 1, "version": 7, "created": "2022-10-05 15:34:59+0900", "updated": "2022-10-06 00:46:35+0900" } ]}

* **total\_count** (32-bit integer): Total number of address groups that match the search keyword
* **address\_groups** (Array): Paged list of address groups that match the search keyword
* **guid** (String): Address group GUID
* **company\_guid** (String): GUID of the company to which the address group belongs
* **company\_name** (String): Name of the company to which the address group belongs
* **name** (String): Address group name
* **description** (String): Address group description
* **count** (32-bit integer): Number of addresses in the address group
* **version** (32-bit integer): Monotonically increasing version number
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### Get Address Group

Retrieves information of a specified address group.

#### HTTP Request

GET /api/sonar/address-groups/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/address-groups/4dc14f3d-ebf8-4032-8a7a-ef9ec6cd3dd2

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Address group GUID | 36 characters |

#### Success Response

{ "address\_group": { "guid": "4dc14f3d-ebf8-4032-8a7a-ef9ec6cd3dd2", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "로그프레소", "name": "방화벽 차단 IP", "description": "차단 연동용 IP 블랙리스트", "count": 1, "version": 7, "created": "2022-10-05 15:34:59+0900", "updated": "2022-10-06 00:46:35+0900" }}

* **address\_group** (Map): Specified address group
* **guid** (String): Address group GUID
* **company\_guid** (String): GUID of the company to which the address group belongs
* **company\_name** (String): Name of the company to which the address group belongs
* **name** (String): Address group name
* **description** (String): Address group description
* **count** (32-bit integer): Number of IP addresses in the address group
* **version** (32-bit integer): Monotonically increasing version number
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)

Address group is not found

HTTP status code 200

{ "address\_group": null}

Identifier is not in valid GUID format

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

### Create Address Group

Creates a new address group.

#### HTTP Request

POST /api/sonar/address-groups

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name=Exceptions \ -X POST \ https://HOSTNAME/api/sonar/address-groups

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| name | O | String | Address group name | Minimum 1 to maximum 50 characters |
| guid | X | String | Address group GUID | 36 characters. The default value is randomly generated. |
| company\_guid | X | String | Company GUID | 36 characters. Default is the GUID of the company in the current session. |
| description | X | String | Address group description | Maximum 2,000 characters |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be shorter than or equal to 50 characters."}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "company\_guid should be guid type."}

Company does not exist

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "company not found: 1245cbbc-681c-4c52-a01b-f4b496d95d50"}

### Update Address Group

Updates a specified address group.

#### HTTP Request

PUT /api/sonar/address-groups/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name=Exceptions \ -d description="Service assets" \ -X PUT \ https://HOSTNAME/api/sonar/address-groups/4dc14f3d-ebf8-4032-8a7a-ef9ec6cd3dd2

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Address group GUID | 36 characters. The default is randomly generated. |
| name | O | String | Address group name | Minimum 1 to maximum 50 characters |
| description | X | String | Address group description | Maximum 2,000 characters |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be shorter than or equal to 50 characters."}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Address group is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "address group not found: 81e7ff9e-457e-4f65-8f8e-bb9b3a0021c8"}

No privileges to update an address group

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Remove Address Groups

Removes the specified address groups.

#### HTTP Request

DELETE /api/sonar/address-groups

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ https://HOSTNAME/api/sonar/address-groups?guids=4dc14f3d-ebf8-4032-8a7a-ef9ec6cd3dd2

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guids | O | String | Address group GUID | Comma-separated list |

#### Success Response

{ "failures": []}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "guids should be not null"}

Invalid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

Failed to delete an address group

HTTP status code 200

{ "failures": [ { "id": "55e6d809-96c8-4d7a-9e20-98e2b34b6cec", "reason": "address-group-not-found" } ]}

No privileges to delete an address group

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Get Address Objects

Gets a list of address objects in a specified address group.

#### HTTP Request

GET /api/sonar/address-groups/:guid/addresses

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/address-groups/8df64276-a16e-4bae-93cd-c207c8155159/addresses

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Address group GUID | 36 characters |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load | Default: 50 |
| keywords | X | String | Keywords | Search available by ip, description |

#### Success Response

{ "total\_count": 1, "addresses": [ { "guid": "d4915ba2-763f-4ec0-a875-38b292a99a24", "ip": "20.214.237.145", "country": "US", "count": 1, "description": "Web app attack", "created": "2022-11-07 01:30:40+0900", "updated": "2022-11-07 01:30:40+0900" } ]}

* **total\_count** (32-bit integer): Total number of addresses that match the search keywords
* **addresses** (Array): Address list
* **guid** (String): Address GUID
* **ip** (String): IP address
* **country** (String): Source country (ISO 2-digit country code)
* **count** (32-bit integer): Hit count
* **description** (String): Description
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### Create Address Object

Creates a new address object for a specified address group.

#### HTTP Request

POST /api/sonar/address-groups/:guid/addresses

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d address=1.1.1.1 \ -d description="Public DNS" \ -X POST \ https://HOSTNAME/api/sonar/address-groups/4dc14f3d-ebf8-4032-8a7a-ef9ec6cd3dd2/addresses

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Address group GUID | 36 characters |
| address | O | String | IP address |  |
| description | X | String | Description | Maximimum 255 characters |
| period | X | 32-bit integer | Retention period in days | Minimum 1 to maximum 52,560,000 |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "address should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'description' must be shorter than or equal to 255 characters."}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Invalid IP address

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "address should be valid IPv4 address: 256.255.255.255"}

Retention period value is less than 1

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'period' must be greater than or equal to 1."}

Retention period value is greater than 52,560,000

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'period' must be less than or equal to 52560000."}

Address group is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "address group not found: ede06992-dd57-4b79-8c54-a295f33d8613"}

No privilege to create an address group

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Remove Address Objects

Removes address objects from a specified address group. Requests for non-existent IP addresses are ignored.

#### HTTP Request

DELETE /api/sonar/address-groups/:guid/addresses

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/address-groups/4dc14f3d-ebf8-4032-8a7a-ef9ec6cd3dd2/addresses?addresses=1.1.1.1"

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Address group GUID | 36 characters |
| addresses | O | String | IP address list | Comma-separated list |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "addresses should be not null"}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Invalid IP address

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "addresses should contain only valid IP addresses. input is 256.255.255.255"}

Address group is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "address group not found: ede06992-dd57-4b79-8c54-a295f33d8613"}

No privileges to delete an address group

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## Subnet Group API

### Get Subnet Groups

Get a list of the subnet groups that match the search keyword.

#### HTTP Request

GET /api/sonar/subnet-groups

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/subnet-groups

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load | If not specified, load all records |
| keywords | X | String | Keyword | Search available by name, description |

#### Success Response

{ "total\_count": 1, "subnet\_groups": [ { "guid": "bb994ca4-1471-4b91-89f2-99a61bd529b5", "name": "Private network", "description": null, "subnet\_count": 3, "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "Admin", "created": "2022-09-01 00:31:14+0900", "updated": "2022-09-01 00:31:14+0900" } ]}

* **total\_count** (32-bit integer): Total number of the subnet groups that match the search keyword
* **subnet\_groups** (Array): Paged list of subnet groups
* **guid** (String): Network subnet group GUID
* **name** (String): Network subnet group name
* **description** (String): Network subnet group description
* **subnet\_count** (32-bit integer): Number of the network subnets that belong to the group
* **company\_guid** (String): GUID of the company (tenant) to which the group belongs.
* **company\_name** (String): Name of the company (tenant) to which the group belongs.
* **user\_guid** (String): GUID of the user who creates the subnet group
* **user\_name** (String): Name of the user who creates the subnet group
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### Get Subnet Group

Retrieves information of a specified subnet group.

#### HTTP Request

GET /api/sonar/subnet-groups/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/subnet-groups/bb994ca4-1471-4b91-89f2-99a61bd529b5

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Subnet group identifier | 36 characters |

#### Success Response

{ "subnet\_group": { "guid": "bb994ca4-1471-4b91-89f2-99a61bd529b5", "name": "Private network", "description": null, "subnet\_count": 3, "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "Admin", "created": "2022-09-01 00:31:14+0900", "updated": "2022-09-01 00:31:14+0900" }}

* **subnet\_group** (Map): Subnet group
* **guid** (String): Subnet group GUID
* **name** (String): Subnet group name
* **description** (String): Subnet group description
* **subnet\_count** (32-bit integer): Number of the subnets that belong to the group
* **company\_guid** (String): GUID of the company (tenant) to which the group belongs.
* **company\_name** (String): Name of the company (tenant) to which the group belongs.
* **user\_guid** (String): GUID of the user who creates the subnet group
* **user\_name** (String): Name of the user who creates the subnet group

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Subnet group is not found

HTTP status code 200

{ "subnet\_group": null}

### Create Subnet Group

Creates a new subnet group.

#### HTTP Request

POST /api/sonar/subnet-groups

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="OA" \ -d description="Office zone" \ -X POST \ https://HOSTNAME/api/sonar/subnet-groups

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | X | String | Subnet group GUID | 36 characters. Randomly generated if not specified. |
| name | O | String | Subnet group name | Minimum 1 to maximum 50 characters |
| description | X | String | Subnet description | Maximum 50 characters |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

Duplicate group name

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "duplicated subnet group name: OA"}

No privilege to create a subnet group

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Update Subnet Group

Updates a specified subnet group.

#### HTTP Request

PUT /api/sonar/subnet-groups/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="OA" \ -d description="Office zone network" \ -X PUT \ https://HOSTNAME/api/sonar/subnet-groups/b76c3c81-c961-404f-a0eb-fae2f12f5bd8

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Subnet group GUID | 36 characters |
| name | O | String | Subnet group name | Minimum 1 to maximum 50 characters |
| description | X | String | Subnet description | Maximum 50 characters |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

Subnet group is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "subnet group not found: c1dfe306-abba-4ed8-862b-0e98e2effcb5"}

Duplicate group name

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "duplicated subnet group name: OA"}

No privileges to update a subnet group

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Remove Subnet Groups

Deletes the specified subnet groups.

#### HTTP Request

DELETE /api/sonar/subnet-groups

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/subnet-groups?guids=638cfeb2-e259-46af-961a-1eeb65ea35f0"

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guids | O | List (of strings) | Subnet group GUID list | Comma-separated list |

#### Success Response

{ "failures": []}

#### Error Responses

Subnet group is not found

HTTP status code 200

{ "failures": [ { "id": "c1dfe306-abba-4ed8-862b-0e98e2effcb6", "reason": "subnet-group-not-found" } ]}

No privileges to delete a subnet group

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Get Subnets

Gets a list of the subnets that belong to a specified subnet group.

#### HTTP Request

GET /api/sonar/subnet-groups/:guid/subnets

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/subnet-groups/bb994ca4-1471-4b91-89f2-99a61bd529b5/subnets

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Subnet group GUID | 36 characters |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load | If not spcified, 20. |
| keywords | X | String | Keyword | Search available by description |

#### Success Response

{ "total\_count": 3, "subnets": [ { "id": 1, "start\_ip": "10.0.0.0", "end\_ip": "10.255.255.255", "cidr": 0, "description": "A class" }, { "id": 2, "start\_ip": "172.16.0.0", "end\_ip": "172.31.255.255", "cidr": 0, "description": null }, { "id": 3, "start\_ip": "192.168.0.0", "end\_ip": "192.168.255.255", "cidr": 0, "description": null } ]}

* **total\_count** (32-bit integer): Total number of the subnet groups that match the search keyword
* **subnets** (Array): Paged list of subnets
* **id** (32-bit integer): Subnet ID
* **start\_ip** (String): Starting IP address
* **end\_ip** (String): Ending IP address
* **cidr** (32-bit integer): CIDR subnet mask value
* **description** (String): Description

#### Error Responses

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### Create Subnet

Create a new subnet for a specified subnet group.

#### HTTP Request

POST /api/sonar/subnet-groups/:guid/subnets

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d start\_ip="192.168.253.1" \ -d end\_ip="192.168.253.255" \ -X POST \ https://HOSTNAME/api/sonar/subnet-groups/b76c3c81-c961-404f-a0eb-fae2f12f5bd8/subnets

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Subnet group GUID | 36 characters |
| start\_ip | O | String | Starting IP address | Minumum 7 to maximum 15 characters |
| end\_ip | X | String | Ending IP address | Minumum 7 to maximum 15 characters |
| cidr | X | 32-bit integer | CIDR | Minimum 0 to maximum 32 |
| description | X | String | Subnet description | Maximum 255 characters |

At least one of `end\_ip` and `cidr` must be provided.

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400.

{ "error\_code": "null-argument", "error\_msg": "start\_ip should be not null"}

Invalid argument length

HTTP status code 400.

{ "error\_code": "invalid-argument", "error\_msg": "'start\_ip' must be less than or equal to 15 characters."}

cidr is not an integer

HTTP status code 400.

{ "error\_code": "invalid-argument", "error\_msg": "'cidr' parameter should be int type"}

No privilege to create a subnet

HTTP status code 500 .

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Update Subnet

Updates the subnet of a specified subnet group.

#### HTTP Request

PUT /api/sonar/subnet-groups/:guid/subnets/:id

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d start\_ip="192.168.253.1" \ -d end\_ip="192.168.253.2" \ -X POST \ https://HOSTNAME/api/sonar/subnet-groups/b76c3c81-c961-404f-a0eb-fae2f12f5bd8/subnets/10

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Subnet group GUID | 36 characters |
| id | O | 32-bit integer | Subnet ID |  |
| start\_ip | O | String | Starting IP address | Minimum 7 to maximum 15characters |
| end\_ip | X | String | Ending IP address | Minimum 7 to maximum 15characters |
| cidr | X | 32-bit integer | CIDR | Minimum 0 to maximum 32 |
| description | X | String | Subnet description | Maximum 255 characters |

At least one of `end\_ip` and `cidr` must be provided.

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400.

{ "error\_code": "null-argument", "error\_msg": "start\_ip should be not null"}

Invalid argument length

HTTP status code 400.

{ "error\_code": "invalid-argument", "error\_msg": "'start\_ip' must be less than or equal to 15 characters."}

cidr value is not an integer

HTTP status code 400.

{ "error\_code": "invalid-argument", "error\_msg": "'cidr' parameter should be int type"}

Subnet group is not found

HTTP status code 500 .

{ "error\_code": "illegal-state", "error\_msg": "subnet group not found: 0c74771b-568e-4696-80ed-6dd4d8b71a12"}

Subnet is not found

HTTP status code 500 .

{ "error\_code": "illegal-state", "error\_msg": "subnet not found: 100"}

No privileges to update a subnet

HTTP status code 500 .

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Remove Subnets

Deletes the specified subnets.

#### HTTP Request

DELETE /api/sonar/subnet-groups/:guid/subnets

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/subnet-groups/638cfeb2-e259-46af-961a-1eeb65ea35f0/subnets?ids=10"

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Subnet group GUID | 36 characters |
| ids | O | List (of 32-bit integers) | Subnet ID list | Comma-separated list |

#### Success Response

{ "failures": []}

#### Error Responses

Subnet group Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Subnet identifier list is not a 32-bit integer list

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'ids' parameter should be int\_list type"}

Subnet is not found

HTTP status code 200

{ "failures": [ { "id": "6", "reason": "subnet-not-found" } ]}

No privileges to delete a subnet

HTTP status code 500 .

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## Pattern Group API

### Get Pattern Groups

Gets a list of the pattern groups that match the search keyword.

#### HTTP Request

GET /api/sonar/pattern-groups

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/pattern-groups

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load |  |
| keywords | X | String | Keyword | Search available by name, description |

#### Success Response

{ "total\_count": 23, "pattern\_groups": [ { "guid": "28ad21b2-585c-4b68-9fad-b78711078496", "name": "IPS WAS Exploit Alert", "description": "Detect attacks that exploit known vulnerabilities in WAS to cause remote code execution, denial of service, etc.", "pattern\_count": 15, "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "Admin", "created": "2022-09-01 00:31:14+0900", "updated": "2022-09-01 00:31:14+0900" } ]}

* **total\_count** (32-bit integer): Total number of the pattern groups that match the search keyword
* **pattern\_groups** (Array): Pattern group list
* **guid** (String): Pattern group GUID
* **name** (String): Pattern group name
* **description** (String): Pattern group description
* **pattern\_count** (32-bit integer): Number of patterns
* **company\_guid** (String): GUID of the company (tenant) to which the group belongs
* **company\_name** (String): Name of the company (tenant) to which the group belongs
* **user\_guid** (String): GUID of the user who creates the pattern group
* **user\_name** (String): Name of the user who creates the pattern group
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### Get Pattern Group

Retrieves information of a specified pattern group.

#### HTTP Request

GET /api/sonar/pattern-groups/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/pattern-groups/28ad21b2-585c-4b68-9fad-b78711078496

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Pattern group identifier | 36 characters |

#### Success Response

{ "pattern\_group": { "guid": "28ad21b2-585c-4b68-9fad-b78711078496", "name": "IPS WAS Exploit Alert", "description": "Detect attacks that exploit known vulnerabilities in WAS to cause remote code execution, denial of service, etc.", "pattern\_count": 15, "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "Admin", "created": "2022-09-01 00:31:14+0900", "updated": "2022-09-01 00:31:14+0900" }}

* **pattern\_group** (Map): Pattern group
* **guid** (String): Pattern group GUID
* **name** (String): Pattern group name
* **description** (String): Pattern group description
* **pattern\_count** (32-bit integer): Number of patterns
* **company\_guid** (String): Identifier of the company (tenant) to which the group belongs
* **company\_name** (String): Name of the company (tenant) to which the group belongs
* **user\_guid** (String): GUID of the user who creates the pattern group
* **user\_name** (String): Name of the user who creates the pattern group
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Pattern group is not found

HTTP status code 200

{ "pattern\_group": null}

### Create Pattern Group

Creates a new pattern group.

#### HTTP Request

POST /api/sonar/pattern-groups

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="Webshell" \ -X POST \ https://HOSTNAME/api/sonar/pattern-groups

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | X | String | Pattern group GUID | 36 characters. Randomly generated if not specified. |
| name | O | String | Pattern group name | Minumum 1 to maximum 50 characters |
| description | X | String | Pattern group description | Maximum 50 characters |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400.

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Invalid argument length

HTTP status code 400.

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

Duplicate pattern group name

HTTP status code 500 .

{ "error\_code": "illegal-state", "error\_msg": "duplicated pattern group name: Webshell"}

No privilege to create a pattern group

HTTP status code 500 .

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Update Pattern Group

Updates a specified pattern group.

#### HTTP Request

PUT /api/sonar/pattern-groups/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="Webshell" \ -d description="Webshell patterns" \ -X PUT \ https://HOSTNAME/api/sonar/pattern-groups

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Pattern group GUID | 36 characters |
| name | O | String | Pattern group name | Minimum 1 to maximum 50 characters |
| description | X | String | Pattern group description | Maximum 50 characters |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 50 characters."}

Pattern group is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "pattern group not found: c1dfe306-abba-4ed8-862b-0e98e2effcb5"}

Duplicated group name

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "duplicated pattern group name: Webshell"}

No privileges to update a pattern group

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Remove Pattern Groups

Deletes the specified pattern groups.

#### HTTP Request

DELETE /api/sonar/pattern-groups

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/pattern-groups?guids=75c80aad-45d5-483a-b771-35bc4609dedc

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guids | O | List (of strings) | Pattern group GUID list | Comma-separated list |

#### Success Response

{ "failures": []}

#### Error Responses

Pattern group is not found

HTTP status code 200

{ "failures": [ { "id": "c1dfe306-abba-4ed8-862b-0e98e2effcb6", "reason": "pattern-group-not-found" } ]}

No privileges to delete a pattern group

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Get Patterns

Get a list of the patterns for a specified pattern group.

#### HTTP Request

GET /api/sonar/pattern-groups/:guid/patterns

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/pattern-groups/8df64276-a16e-4bae-93cd-c207c8155159/patterns

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Pattern group GUID | 36 characters |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load | If not sepcified, 20 |
| keywords | X | String | Keyword | Search available by rule, expr, expr2 |

#### Success Response

{ "total\_count": 2, "patterns": [ { "id": 112, "expr": "\"passwd\"", "expr2": "path == \"\*passwd\"", "rule": "/etc/passwd", "created": "2022-09-01 00:31:14+0900", "updated": "2022-09-01 00:31:14+0900" }, { "id": 113, "expr": "\"authorized\_keys\"", "expr2": "path == \"\*authorized\_keys\"", "rule": "/.ssh/authorized\_keys", "created": "2022-09-01 00:31:14+0900", "updated": "2022-09-01 00:31:14+0900" } ]]

* **total\_count** (32-bit integer): Total number of the patterns that match the search keyword
* **patterns** (Array): Pattern list
* **id** (32-bit integer): Pattern ID
* **expr** (String): Keyword boolean expression
* **expr2** (String): Validation expression that filters the keyword-matching result
* **rule** (String): Pattern name
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### Create Pattern

Create a new pattern for a specified pattern group.

#### HTTP Request

POST /api/sonar/pattern-groups/:guid/patterns

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d expr="""/.git/HEAD""" \ -d rule="/.git/HEAD file scan" \ -X POST \ https://HOSTNAME/api/sonar/pattern-groups/e93dafa7-6215-4e98-8bfc-1e0a67171bf1/patterns

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Pattern group GUID | 36 characters |
| expr | O | String | Keyword boolean expression | Minimum 3 to maximum 1,000 characters |
| expr2 | X | String | Validation expression | Maximum 1,000 characters |
| rule | O | String | Pattern name | Maximum 1,000 characters |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400.

{ "error\_code": "null-argument", "error\_msg": "expr should be not null"}

Invalid argument length

HTTP status code 400.

{ "error\_code": "invalid-argument", "error\_msg": "'expr' must be less than or equal to 1000 characters."}

Invalid keyword boolean expression

HTTP status code 400.

{ "error\_code": "invalid-argument", "error\_msg": "expr syntax error: not-quoted"}

No privilege to create a pattern

HTTP status code 500 .

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Update Pattern

Updates the pattern of a specified pattern group.

#### HTTP Request

PUT /api/sonar/pattern-groups/:guid/patterns/:id

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d expr=""/.git/HEAD"" \ -d expr2="path == ""\*/.git/HEAD""" \ -d rule="/.git/HEAD file scan" \ -X PUT \ https://HOSTNAME/api/sonar/pattern-groups/e93dafa7-6215-4e98-8bfc-1e0a67171bf1/patterns/

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Pattern group GUID | 36 characters |
| expr | O | String | Keyword boolean expression | Minimim 3 to maximum 1,000 characters |
| expr2 | X | String | Validation expression | Maximum 1,000 characters |
| rule | O | String | Pattern name | Maximum 1,000 characters |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "expr should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'expr' must be less than or equal to 1000 characters."}

Invalid keyword boolean expression

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "expr syntax error: not-quoted"}

No privileges to update a pattern

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Remove Patterns

Deletes the specified patterns.

#### HTTP Request

DELETE /api/sonar/pattern-groups/:guid/patterns

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/pattern-groups/638cfeb2-e259-46af-961a-1eeb65ea35f0/pattern?ids=10"

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Pattern group GUID | 36 characters |
| ids | O | List (of 32-bit integers) | Pattern ID list | Comma-separated list |

#### Success Response

{ "failures": []}

#### Error Responses

Pattern group identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Pattern identifiers list is not a 32-bit integer list

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'ids' parameter should be int\_list type"}

Pattern is not found

HTTP status code 200

{ "failures": [ { "id": "6", "reason": "pattern-not-found" } ]}

No privileges to delete a pattern

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## Table API

### Get Tables

Gets a list of the tables that match the search keyword.

Even on the same instance, configuration information for tables created in Logpresso Enterprise is not retrieved because it does not exist in Logpresso Sonar.

#### HTTP Request

GET /api/sonar/tables

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/tables

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load | Default: 2147483647 |
| keywords | X | String | Keyword | Search available by table\_name |
| company\_guid | X | String | Company GUID | Option only available for a cluster administrator |

#### Success Response

{ "total\_count": 1, "tables": [ { "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "table\_name": "evtx\_system", "layout": "columnar", "compression": "snappy", "retention": 180, "min\_day": "2021-10-19 00:00:00+0900", "max\_day": "2022-09-14 00:00:00+0900", "table\_size": 7195337, "index\_size": 0, "ratio": 100 } ]}

* **total\_count** (32-bit integer): Total number of tables that match the search keyword
* **tables** (Array): Table list
* **company\_guid** (String): Company (tenant) GUID
* **company\_name** (String): Company (tenant) name
* **table\_name** (String): Table name
* **layout** (String): Block layout
* **compression** (String): Compression algorithm
* **crypto\_profile\_guid** (String): Encryption profile GUID
* **crypto\_profile\_name** (String): Encryption profile name
* **min\_day** (String): Minimum log date stored (based on \_time field)
* **max\_day** (String): Maximum log date stored (based on \_time field)
* **table\_size** (64-bit integer): Table data size (Bytes)
* **index\_size** (64-bit integer): Index data size (Bytes)
* **retention** (32-bit integer): Data retention period (in days)
* **ratio** (64-bit real number): Storage usage ratio

#### Error Responses

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "company\_guid should be guid type."}

### Get Table

Retrieves configuration and status information of a specified table.

Even on the same instance, configuration information for tables created in Logpresso Enterprise is not retrieved because it does not exist in Logpresso Sonar.

#### HTTP Request

GET /api/sonar/tables/:table

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/tables/demo

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| table | O | String | Table name | Case-sensitive. Minimum 1 to maximum 50 characters |

Table names can only contain numbers, upper and lower case alphabets, and underscores.

#### Success Response

{ "table": { "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "table\_name": "evtx\_system", "layout": "columnar", "compression": "snappy", "retention": 180, "table\_size": 7731856, "index\_size": 10645038, "ratio": 100, "min\_day": "2021-10-19 00:00:00+0900", "max\_day": "2022-09-14 00:00:00+0900", "shared\_users": [ { "type": "USER", "guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "name": "Joshua", "read\_only": true, "created": "2022-09-11 21:57:20+0900" } ], "shared\_groups": [], "node\_stats": [ { "node\_pair\_name": "control", "table\_size": 7731856, "index\_size": 10645038, "min\_day": "2021-10-19 00:00:00+0900", "max\_day": "2022-09-14 00:00:00+0900" } ] }}

* **table** (Map): Tabele configurations
* **company\_guid** (String): Company (tenant) GUID
* **company\_name** (String): Company (tenant) name
* **table\_name** (String): Table name
* **layout** (String): Block layout
* **compression** (String): Compression algorithm
* **retention** (32-bit integer): Data retention period (days)
* **crypto\_profile\_guid** (String): Encryption profile GUID
* **crypto\_profile\_name** (String): Encryption profile name
* **table\_size** (64-bit integer): Table data size (Bytes)
* **index\_size** (64-bit integer): Index data size (Bytes)
* **ratio** (64-bit real number): Ratio of disk usage for the table to the disk usage of all tables.
* **min\_day** (String): Minimum log date stored (based on \_time field)
* **max\_day** (String): Maximum log date stored (based on \_time field)
* **shared\_users** (Array): List of the users with privilege for the table
* **type** (String): Always USER
* **guid** (String):
* **shared\_groups** (Array): List of the user groups with privilege for the table
* **node\_stats** (Array): Table statistics information by nodes
* **node\_pair\_name** (String): Node pair name
* **table\_size** (64-bit integer): Table data size
* **index\_size** (64-bit integer): Index data size
* **min\_day** (String): Minimum log date stored (based on \_time field)
* **max\_day** (String): Maximum log date stored (based on \_time field)

#### Error Response

Table is not found

HTTP status code 200

{ "table": null}

### Create Table

Creates a new Logpresso Sonar table. Administrator privileges are required to call this API.

#### HTTP Request

POST /api/sonar/tables

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d table=demo \ -d company\_guid=6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311 \ -X POST \ https://HOSTNAME/api/sonar/tables

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| table | O | String | Table name | Case-sensitive. Minimum 1 to maximum 50 characters |
| company\_guid | O | String | Company GUID | 36 characters |
| compression | X | String | Compression algorithm | Default: snappy |
| layout | X | String | Block layout | Default: columnar |
| crypto\_profile\_guid | X | String | Encryption profile GUID | 36 characters |
| retention | X | 32-bit integer | Retention cycle in days | Minimum: 0 (unlimitied). Maximum: 36500. Default: 0 |

Table names can only contain numbers, upper and lower case alphabets, and underscores.

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "table should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'table' must be shorter than or equal to 50 characters."}

Invalid table name

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'table' must begin with a letter and may contain alphanumeric and underscore characters: 0123"}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "company\_guid should be guid type."}

Invalid compression algorithm

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'compression' should be one of deflate or snappy."}

Invalid block layout

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'layout' should be one of row or columnar."}

Retention period out of valid range

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'retention' must be less than or equal to 36500."}

No privilege to create a table

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

Duplicate table name

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "duplicated table name: demo"}

Company is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "company not found: 6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa312"}

Crypto profile is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "crypto profile not found: 6f238ab0-7c11-4dc3-9543-ebb3d1cdde12"}

### Drop Table

Drops a specified table. Company (tenant) or higher privileges are required to call this API.

#### HTTP Request

DELETE /api/sonar/tables/:table

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE https://HOSTNAME/api/sonar/tables/demo

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| table | O | String | Table name | Case-sensitive. Minimum 1 to maximum 50 characters |

Table names can only contain numbers, upper and lower case alphabets, and underscores.

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "table should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'table' must be shorter than or equal to 50 characters."}

Invalid table name

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'table' must begin with a letter and may contain alphanumeric and underscore characters: 0123"}

No privilege to delete a table

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

Table is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "table not found: test"}

### Drop Table Partitions

Drops the table data within a specified period. Administrator privileges are required to call this API.

#### HTTP Request

DELETE /api/sonar/tables/:table/partitions

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE "https://HOSTNAME/api/sonar/tables/demo/partitions?start=2022-01-01&end=2022-12-31"

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| table | O | String | Table name | Case-sensitive. Minimum 1 to maximum 50 characters |
| start | O | String | Start date | yyyy-MM-dd format |
| end | O | String | End date | yyyy-MM-dd format. The end date is included in the range. |

Table names can only contain numbers, upper and lower case alphabets, and underscores.

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "start should be not null"}

Invalid date format

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'end' should be yyyy-MM-dd format."}

Start date is later than end date

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "date range is unacceptable."}

Invalid table name

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'table' must begin with a letter and may contain alphanumeric and underscore characters: 0123"}

No privileges to drop table partition

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

Table is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "table not found: test"}

### Set Table Retention

#### HTTP Request

PUT /api/sonar/tables/:table/retention

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X PUT \ "https://HOSTNAME/api/sonar/tables/demo/retention?period=180"

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| table | O | String | Table name | Case-sensitive. Minimum 1 to maximum 50 characters |
| period | O | 32-bit integer | Retention period (days) | Minimum: 0 (unlimited), Maximum: 36500 |

Table names can only contain numbers, upper and lower case alphabets, and underscores.

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "period should be not null"}

Retention period out of valid range

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'period' must be less than or equal to 36500."}

Table is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "table not found: test"}

### Get Procedures

Gets a list of the procedures that match the search keyword.

#### HTTP Request

GET /api/sonar/procedures

#### Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/procedures

#### Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Requied | Type | Description | Note |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load | Default: all procedures |
| keywords | X | String | Search keyword | Search available by name, description |

#### Success Response

{ "total\_count": 1, "procedures": [ { "guid": "5ad13151-dbc1-41c0-92a7-dfeb5f534f4c", "name": "test", "description": null, "parameters": [ { "name": "테이블", "description": "검색 대상 테이블 이름", "type": "string", "key": "table" } ], "query": "system tables | search table == $(\"table\")", "owner\_guid": "13437402-81ed-4b6c-8a6f-7893c7c958b1", "owner\_name": "데모", "owner\_login\_name": "demo", "company\_public": false, "created": "2023-10-03 12:38:13+0900", "updated": "2023-10-03 22:14:28+0900" } ]}

This API does not return the information of granted users or groups.

* **total\_count** (32-bit integer): Total number of the procedures that match the search keyword
* **procedures** (Array): List of procedures
* **guid** (String): Procedure identifier
* **name** (String): Procedure name
* **description** (String): Procedure description
* **parameters** (Array): Parameter list
* **name** (String): Display name of the parameter
* **description** (String): Description of the parameter
* **type** (String): Parameter type. Either string, int, double, bool, datetime, date, or ip.
* **key** (String): Parameter name
* **query** (String): Query string
* **owner\_guid** (String): Owner GUID as identifier
* **owner\_name** (String): Owner name
* **owner\_login\_name** (String): Owner login account
* **company\_public** (Boolean): Whether the procedure is public
* **created** (String): Creation date and time (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Last modification date and time (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### Get Procedure

Retrieves information of a specified procedure.

#### HTTP Request

GET /api/sonar/procedures/:guid

#### Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/procedures/5ad13151-dbc1-41c0-92a7-dfeb5f534f4c

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Requied | Type | Description | Note |
| guid | O | String | Procedure identifier | 36 charaters |

#### Success Response

{ "procedure": { "guid": "5ad13151-dbc1-41c0-92a7-dfeb5f534f4c", "name": "test", "description": null, "parameters": [ { "name": "테이블", "description": "검색 대상 테이블 이름", "type": "string", "key": "table" } ], "query": "system tables | search table == $(\"table\")", "owner\_guid": "13437402-81ed-4b6c-8a6f-7893c7c958b1", "owner\_name": "데모", "owner\_login\_name": "demo", "company\_public": false, "granted\_users": [ { "guid": "b5bc3133-b53e-4b61-96b5-8857015ade0d", "name": "demo2", } ], "granted\_groups": [], "created": "2023-10-03 12:38:13+0900", "updated": "2023-10-03 22:15:28+0900" }}

* **total\_count** (32-bit integer): Total number of the procedures that match the search keyword
* **procedures** (Array): List of procedures
* **guid** (String): Procedure identifier
* **name** (String): Procedure name
* **description** (String): Procedure description
* **parameters** (Array): Parameter list
* **name** (String): Display name of the parameter
* **description** (String): Description of the parameter
* **type** (String): Parameter type. Either string, int, double, bool, datetime, date, or ip.
* **key** (String): Parameter name
* **query** (String): Query string
* **owner\_guid** (String): Owner GUID as identifier
* **owner\_name** (String): Owner name
* **owner\_login\_name** (String): Owner login account
* **company\_public** (Boolean): Whether the procedure is public
* **granted\_users** (Array):
* **guid** (String): User GUID as identifier
* **name** (String): User name
* **granted\_groups** (Array):
* **guid** (String): Group GUID as identifier
* **name** (String): Group name
* **created** (String): Creation date and time (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Last modification date and time (yyyy-MM-dd HH:mm:ssZ)

### Create Procedure

Creates a new procedure.

#### HTTP Request

POST /api/sonar/procedures

#### Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="test" \ -d 'query=system tables | search table == $("table")' \ -d 'parameters=[{"type": "string", "name": "테이블", "key": "table"}]' \ -d granted\_user\_guids=b5bc3133-b53e-4b61-96b5-8857015ade0d \ -X POST https://HOSTNAME/api/sonar/procedures

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Requied | Type | Description | Note |
| guid | X | String | Procedure identifier | 36 characters. If not specified, randomly generated. |
| name | O | String | Procedure name | Minimum 1 to maximum 2,000 characters |
| description | X | String | Procedure description | Maximum 2,000 characters |
| query | O | String | Query string |  |
| parameters | X | Object Array | Parameter list | Including type, key, name, description |
| company\_public | X | Boolean | Whether the procedure is public |  |
| granted\_user\_guids | X | String Array | List of granted user GUIDs | Comma-separated GUID list |
| granted\_group\_guids | X | String Array | List of granted user group GUIDs | Comma-separated GUID list |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 255 characters."}

User or group identifier is not in valid GUID format

{ "error\_code": "invalid-param-type", "error\_msg": "granted\_user\_guids should be guid type."}

### Update Procedure

Updates a specified procedure.

#### HTTP Request

PUT /api/sonar/procedures/:guid

#### Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="test" \ -d 'query=system tables | search table == $("table")' \ -d 'parameters=[{"type": "string", "name": "테이블", "key": "table"}]' \ -d granted\_user\_guids=b5bc3133-b53e-4b61-96b5-8857015ade0d \ -X PUT https://HOSTNAME/api/sonar/procedures/5ad13151-dbc1-41c0-92a7-dfeb5f534f4c

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Requied | Type | Description | Note |
| guid | O | String | Procedure identifier | 36 characters |
| name | O | String | Procedure name | Minimum 1 to maximum 2,000 characters |
| description | X | String | Procedure description | Maximum 2,000 characters |
| query | O | String | Query string |  |
| parameters | X | Object Array | Parameter list | Including type, key, name, description |
| company\_public | X | Boolean | Whether the procedure is public | Default: false |
| granted\_user\_guids | X | String Array | List of granted user GUIDs | Comma-separated GUID list |
| granted\_group\_guids | X | String Array | List of granted user group GUIDs | Comma-separated GUID list |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be less than or equal to 255 characters."}

User or group identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "granted\_user\_guids should be guid type."}

### Remove Procedures

Removes specified procedures.

#### HTTP Request

DELETE /api/sonar/procedures

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids=5ad13151-dbc1-41c0-92a7-dfeb5f534f4c \ -X DELETE https://HOSTNAME/api/sonar/procedures

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Requied | Type | Description | Note |
| guids | O | List of Strings | Procedure identifier list | Comma-separated GUID list |

#### Success Response

{ "failures": []}

#### Error Responses

Procedure is not found

HTTP status code 200

{ "failures": [ { "id": "c1dfe306-abba-4ed8-862b-0e98e2effcb6", "reason": "procedure-not-found" } ]}

No administrative privilege

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## Stream Rule API

### Get Stream Rules

Gets a list of the stream rules that match the search keyword.

#### HTTP Request

GET /api/sonar/stream-rules

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/stream-rules

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load | If not specified, load all records |
| keywords | X | String | Keyword | Search available by name, description, query target |

#### Success Response

Below is a portion of the full list of stream rules.

{ "total\_count": 52, "rules": [ { "priority": "LOW", "guid": "3b05608f-8dd0-4218-9d6d-391515b6280d", "name": "Disabling Windows Firewall", "description": "(T1089) Disabling Security Tools\n(T1047) Windows Management Instrumentation ", "msg": "Disabling Windows Firewall: $primary\_ip", "enabled": false, "category\_guid": "aedc65d6-25ee-4d9e-9040-e21ebe823f8d", "category\_name": "Evasion", "schema\_code": "edr-process", "schema\_name": "EDR Processs", "logger\_guids": [], "commands": [ { "template\_id": 1, "field\_name": "", "args": {}, "query": "search (lower(image) == \"\*\\\\netsh.exe\" and lower(cmd\_line) == \"\*advfirewall\*\" and lower(cmd\_line) == \"\*off\*\") or (lower(image) == \"\*\\\\netsh.exe\" and lower(cmd\_line) == \"\*firewall\*\" and lower(cmd\_line) == \"\*disable\*\")", "invert": false, "ordinal": 0 } ], "address\_group\_guid": null, "address\_field": null, "ticket\_repo\_guid": null, "ticket\_assignee\_guid": null, "ticket\_assignee\_name": null, "ticket\_suppress\_interval": 3600, "event\_suppress\_interval": 0, "suppress\_key": null, "keep\_alive": false, "audit\_category\_guid": null, "audit\_category\_name": null, "auditor\_guid": null, "auditor\_name": null, "audit\_days": 14, "employee\_key\_field": null, "alarm\_group\_guid": null, "alarm\_group\_name": null, "field\_order": "cmd\_line, image", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "Admin", "created": "2022-09-01 00:31:15+0900", "updated": "2022-09-01 00:31:15+0900" } ]}

* **total\_count** (32-bit integer): Total number of stream rules that match the search keyword
* **rules** (Array): Paged list of stream rules
* **priority** (String): One of the following: LOW, MEDIUM, HIGH.
* **guid** (String): Stream rule GUID
* **name** (String): Stream rule name
* **description** (String): Stream rule description
* **msg** (String): Message template. Macro in the $field format available.
* **enabled** (Boolean): Whether the rule is enabled or not
* **category\_guid** (String): Stream rule category GUID
* **category\_name** (String): Stream rule category name
* **schema\_code** (String): Log schema code
* **schema\_name** (String): Log schema name
* **logger\_guids** (Array): Logger GUID list
* **commands** (Array): List of stream rule commands
* **template\_id** (32-bit integer): Stream rule command template ID
* **field\_name** (String): Target field name
* **args** (Map): Argument key/value pairs
* **query** (String): Query string with arguments
* **invert** (Boolean): NOT condition when invert = true
* **ordinal** (32-bit integer): Order
* **address\_group\_guid** (String): Address group GUID
* **address\_field** (String): Target fields to add to the address group
* **ticket\_repo\_guid** (String): Ticket repository GUID
* **ticket\_assignee\_guid** (String): Ticket assignee GUID
* **ticket\_assignee\_name** (String): Ticket assignee name
* **ticket\_suppress\_interval** (32-bit integer): Suppression period for duplicated ticket in seconds (in seconds)
* **event\_suppress\_interval** (32-bit integer): Suppression period for duplicated event in seconds (in seconds)
* **suppress\_key** (String): Suppress key field. Macro in the $field format available.
* **keep\_alive** (Boolean): true to keep the timer alive, false to reset it.
* When keeping the suppression timer, even if a user completes the ticket, the event will be merged into the existing ticket until the expiration time is reached.
* **audit\_category\_guid** (String): Audit category GUID
* **audit\_category\_name** (String): Audit category name
* **auditor\_guid** (String): Auditor GUID. If not specified, the department head is assigned as default.
* **auditor\_name** (String): Auditor name. If not specified, the department head is assigned as default.
* **audit\_days** (32-bit integer): Audit due date (days)
* **employee\_key\_field** (String): Employee number field. Typically using a normalized emp\_key field.
* **alarm\_group\_guid** (String): Alarm group GUID
* **alarm\_group\_name** (String): Alarm group name
* **field\_order** (String): Evidence file output order. Comma-separated list of field names.
* **company\_guid** (String): GUID of the company (tenant) to which the stream rule belongs
* **company\_name** (String): Name of the company (tenant) to which the stream rule belongs
* **user\_guid** (String): GUID of the user who creates the stream rule
* **user\_name** (String): Name of the user who creates the stream rule
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### Get Stream Rule

Retrieves information of a specified stream rule.

#### HTTP Request

GET /api/sonar/stream-rules/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/stream-rules/3b05608f-8dd0-4218-9d6d-391515b6280d

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Stream rule GUID | 36 characters |

#### Success Response

{ "rule": { "priority": "LOW", "guid": "3b05608f-8dd0-4218-9d6d-391515b6280d", "name": "Disabling Windows Firewall", "description": "(T1089) Disabling Security Tools\n(T1047) Windows Management Instrumentation ", "msg": "Disabling Windows Firewall: $primary\_ip", "enabled": false, "category\_guid": "aedc65d6-25ee-4d9e-9040-e21ebe823f8d", "category\_name": "Evasion", "schema\_code": "edr-process", "schema\_name": "EDR Process", "extractors": [], "commands": [ { "template\_id": 1, "field\_name": "", "args": {}, "query": "search (lower(image) == \"\*\\\\netsh.exe\" and lower(cmd\_line) == \"\*advfirewall\*\" and lower(cmd\_line) == \"\*off\*\") or (lower(image) == \"\*\\\\netsh.exe\" and lower(cmd\_line) == \"\*firewall\*\" and lower(cmd\_line) == \"\*disable\*\")", "invert": false, "ordinal": 0 } ], "address\_group\_guid": null, "address\_field": null, "ticket\_repo\_guid": null, "ticket\_assignee\_guid": null, "ticket\_assignee\_name": null, "ticket\_suppress\_interval": 3600, "event\_suppress\_interval": 0, "suppress\_key": null, "keep\_alive": false, "audit\_category\_guid": null, "audit\_category\_name": null, "auditor\_guid": null, "auditor\_name": null, "audit\_days": 14, "employee\_key\_field": null, "alarm\_group\_guid": null, "alarm\_group\_name": null, "field\_order": "cmd\_line, image", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "Admin", "created": "2022-09-01 00:31:15+0900", "updated": "2022-09-01 00:31:15+0900" }}

* **rule** (Map): Stream rule
* **priority** (String): One of the following: LOW, MEDIUM, HIGH.
* **guid** (String): Stream rule GUID
* **name** (String): Stream rule name
* **description** (String): Stream rule description
* **msg** (String): Message template. Macro in the $field format available.
* **enabled** (Boolean): Whether the rule is enabled or not
* **category\_guid** (String): Stream rule category GUID
* **category\_name** (String): Stream rule category name
* **schema\_code** (String): Log schema code
* **schema\_name** (String): Log schema name
* **logger\_guids** (Array): Logger GUID list
* **commands** (Array): List of stream rule commands
* **template\_id** (32-bit integer): Stream rule command template ID
* **field\_name** (String): Target field name
* **args** (Map): Argument key/value pairs
* **query** (String): Query string with arguments
* **invert** (Boolean): NOT condition when invert = true
* **ordinal** (32-bit integer): Order
* **address\_group\_guid** (String): Address group GUID
* **address\_field** (String): Target fields to add to the address group
* **ticket\_repo\_guid** (String): Ticket repository GUID
* **ticket\_assignee\_guid** (String): Ticket assignee GUID
* **ticket\_assignee\_name** (String): Ticket assignee name
* **ticket\_suppress\_interval** (32-bit integer): Suppression period for duplicated ticket in seconds (in seconds)
* **event\_suppress\_interval** (32-bit integer): Suppression period for duplicated event in seconds (in seconds)
* **suppress\_key** (String): Suppress key field. Macro in the $field format available.
* **keep\_alive** (Boolean): true to keep the timer alive, false to reset it.
* When keeping the suppression timer, even if a user completes the ticket, the event will be merged into the existing ticket until the expiration time is reached.
* **audit\_category\_guid** (String): Audit category GUID
* **audit\_category\_name** (String): Audit category name
* **auditor\_guid** (String): Auditor GUID. If not specified, the department head is assigned as default.
* **auditor\_name** (String): Auditor name. If not specified, the department head is assigned as default.
* **audit\_days** (32-bit integer): Audit due date (days)
* **employee\_key\_field** (String): Employee number field. Typically using a normalized emp\_key field.
* **alarm\_group\_guid** (String): Alarm group GUID
* **alarm\_group\_name** (String): Alarm group name
* **field\_order** (String): Evidence file output order. Comma-separated list of field names.
* **company\_guid** (String): GUID of the company (tenant) to which the stream rule belongs
* **company\_name** (String): Name of the company (tenant) to which the stream rule belongs
* **user\_guid** (String): GUID of the user who creates the stream rule
* **user\_name** (String): Name of the user who creates the stream rule
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

Stream rule is not found

HTTP status code 200

{ "rule": null}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

### Create Stream Rule

Creates a new stream rule.

#### HTTP Request

POST /api/sonar/stream-rules

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d priority="HIGH" \ -d name="Access to known botnet networks" \ -d msg="Access to known botnet networks: $dst\_ip" \ -d schema\_code="session" \ -d commands="[{'template\_id': 3, 'query': 'matchnet invert=t field=dst\_ip guid=697393b6-aecf-4e9d-a32c-8724cd8f067e verify=f', 'field\_name': 'dst\_ip', 'args':{'subnet':'697393b6-aecf-4e9d-a32c-8724cd8f067e'}}]" \ -X POST \ https://HOSTNAME/api/sonar/stream-rules

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| priority | O | String | Priority | LOW or MEDIUM or HIGH. |
| guid | X | String | Stream rule GUID | 36 characters |
| name | O | String | Stream rule name | Minimum 1 to maximum 255 characters |
| description | X | String | Stream rule description | Maximum 2,000 characters |
| msg | O | String | Message template | Minimum 1 to maximum 2,000 characters |
| enabled | X | Boolean | Whether the stream rule is enabled or not | true or false |
| category\_guid | X | String | Stream rule category GUID | 36 characters |
| schema\_code | O | String | Log schema code | Minimum 1 to maximum 50 characters |
| logger\_guids | O | Array | Logger GUID list |  |
| commands | O | Array | List of stream rules | At least one command required. Refer to the below description. |
| address\_group\_guid | X | String | Address group GUID | 36 characters |
| address\_field | X | String | Address field | Address group field name. Maximum 50 characters. |
| ticket\_repo\_guid | X | String | Ticket repository GUID | 36 characters. If not specified, a ticket is not generated. |
| ticket\_assignee\_guid | X | String | Ticket assignee GUID | If specified, ticket is assigned automatically. |
| ticket\_suppress\_interval | X | 32-bit integer | Suppression period for duplicated ticket (in seconds) | If set to 0 or not specified, duplicate tickets are not merged. |
| event\_suppress\_interval | X | 32-bit integer | Suppression period for duplicated event (in seconds) | If set to 0 or not specified, duplicate events are not merged. |
| suppress\_key | X | String | Suppress key field | Maximum 2,000 characters. Macro in $field format available. |
| keep\_alive | X | Boolean | Whether to keep the suppression timer alive | true to keep the timer alive, false to reset it. |
| audit\_category\_guid | X | String | Audit category GUID | 36 characters. If not specified, an auto audit request is not sent. |
| auditor\_guid | X | String | Auditor GUID | 36 characters. If not specified, the department head is assigned as default. |
| audit\_days | X | 32-bit integer | Audit due date | Minimum 1 to maximum 365 days |
| employee\_key\_field | X | String | Employee number field | Maximum 50 characters. If not specified, an auto audit request is not sent. |
| alarm\_group\_guid | X | String | Alarm group GUID | 36 characters |
| field\_order | X | String | Evidence field output order | Maximum 2,000 characters |

Each array element in commands is defined as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| template\_id | O | 32-bit integer | Stream rule command template ID |  |
| query | O | String | Query string portion |  |
| field\_name | X | String | Target field name |  |
| args | X | Map | Argument key/value |  |
| invert | X | Boolean | Whether to use an invert match option |  |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "schema\_code should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'schema\_code' must be shorter than or equal to 50 characters."}

Invalid priority value

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "priority should be one of 'LOW', 'MEDIUM', 'HIGH'."}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "category\_guid should be guid type."}

List of stream rules is not in valid JSON format

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'commands' parameter should follow valid JSON syntax"}

Log schema is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "schema not found: unknown"}

No privilege to create a stream rule

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Update Stream Rule

Updates a specified stream rule.

#### HTTP Request

PUT /api/sonar/stream-rules/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d priority="MEDIUM" \ -d name="Access to known botnet networks" \ -d msg="Access to known botnet networks: $dst\_ip" \ -d schema\_code="session" \ -d commands="[{'template\_id': 3, 'query': 'matchnet invert=t field=dst\_ip guid=697393b6-aecf-4e9d-a32c-8724cd8f067e verify=f', 'field\_name': 'dst\_ip', 'args':{'subnet':'697393b6-aecf-4e9d-a32c-8724cd8f067e'}}]" -X PUT \ https://HOSTNAME/api/sonar/stream-rules/5a6b63f0-87d5-49c4-a5a1-94da4141b2f5

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| priority | O | String | Priority | LOW or MEDIUM or HIGH |
| guid | O | String | Stream rule GUID | 36 characters |
| name | O | String | Stream rule name | Minimum 1 to maximum 255 characters |
| description | X | String | Stream rule Description | Maximum 2,000 characters |
| msg | O | String | Message template | Minimum 1 to maximum 2,000 characters |
| enabled | X | Boolean | Whether the rule is enabled or not | true or false |
| category\_guid | X | String | Stream rule category GUID | 36 characters |
| schema\_code | O | String | Log schema code | Minimum 1 to maximum 50 characters |
| logger\_guids | O | Array | Logger GUID list |  |
| commands | O | Array | List of stream rules | At leat 1 command required. Refer to the below description. |
| address\_group\_guid | X | String | Address group GUID | 36 characters |
| address\_field | X | String | Address field | Address group field name. Maximum 50 characters. |
| ticket\_repo\_guid | X | String | Ticket repository GUID | 36 characters. If not specified, a ticket is not generated. |
| ticket\_assignee\_guid | X | String | Ticket assignee GUID | If specified, ticket is assigned automatically. |
| ticket\_suppress\_interval | X | 32-bit integer | Suppression period for duplicated ticket in seconds | If set to 0 or not specified, duplicate tickets are not merged. |
| event\_suppress\_interval | X | 32-bit integer | Suppression period for duplicated event in seconds | If set to 0 or not specified, duplicate events are not merged. |
| suppress\_key | X | String | Suppress key field | Macro in $field format available. Max. 2,000 characters |
| keep\_alive | X | Boolean | Whether to keep the suppression timer alive | true to keep the timer alive, false to reset it. |
| audit\_category\_guid | X | String | Audit category GUID | 36 characters. If not specified, an auto audit request is not sent. |
| auditor\_guid | X | String | Auditor GUID | 36 characters. If not specified, the department head is assigned as default. |
| audit\_days | X | 32-bit integer | Audit due date | Minimum 1 to maximum 365 days |
| employee\_key\_field | X | String | Employee number field | Maximum 50 characters. If not specified, an auto audit request is not sent. |
| alarm\_group\_guid | X | String | Alarm group GUID | 36 characters |
| field\_order | X | String | Evidence field output order | Maximum 2,000 characters |

Each array element in commands is as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| template\_id | O | 32-bit integer | Stream rule command template ID |  |
| query | O | String | Query string portion |  |
| field\_name | X | String | Target field name |  |
| args | X | Map | Argument key/value |  |
| invert | X | Boolean | Whether to use an invert match option |  |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "schema\_code should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'schema\_code' must be shorter than or equal to 50 characters."}

Invalid priority value

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "priority should be one of 'LOW', 'MEDIUM', 'HIGH'."}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "category\_guid should be guid type."}

List of stream rule commands is not in valid JSON format

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'commands' parameter should follow valid JSON syntax"}

Stream rule is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "stream rule not found: 9071a6fe-6b91-4448-9761-7123381cb026"}

Log schema is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "schema not found: unknown"}

No privilege to create a stream rule

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Remove Stream Rules

Deletes the specified stream rules.

#### HTTP Request

DELETE /api/sonar/stream-rules

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/stream-rules?guids=638cfeb2-e259-46af-961a-1eeb65ea35f0"

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guids | O | List (of strings) | Stream rule GUID list | Comma-separated list |

#### Success Response

{ "failures": []}

#### Error Responses

Stream rule is not found

HTTP status code 200

{ "failures": [ { "id": "638cfeb2-e259-46af-961a-1eeb65ea35f1", "reason": "stream-rule-not-found" } ]}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

### Enable Stream Rule

Enables a specified stream rule.

#### HTTP Request

POST /api/sonar/stream-rules/:guid/enable

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/stream-rules/4f2fe6ea-7c96-4529-88db-2ddf09ce1fa2/enable

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Stream rule GUID | 36 characters |

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Stream rule is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "stream rule not found: 05efb651-9644-4518-950f-dbd648c973a7"}

Stream rule is already enabled

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "stream rule is already enabled: 64bf7657-6f0c-4c14-b0b2-d455263d9205"}

No privileges to enable a stream rule

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Disable Stream Rule

Disables a specified stream rule.

#### HTTP Request

POST /api/sonar/stream-rules/:guid/disable

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/stream-rules/4f2fe6ea-7c96-4529-88db-2ddf09ce1fa2/disable

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Stream rule GUID | 36 characters |

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Stream rule is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "stream rule not found: 05efb651-9644-4518-950f-dbd648c973a7"}

Stream rule is already disabled

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "stream rule is already disabled: 64bf7657-6f0c-4c14-b0b2-d455263d9205"}

No privileges to disable a stream rule

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Get Stream Rule Command Templates

Retrieves a list of all stream rule command templates.

The stream rule command template is to support GUI-style editing of stream rules.

#### HTTP Request

GET /api/sonar/stream-rule-command-templates

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/stream-rule-command-templates

#### Success Response

Below is a portion of the full list of real-time detection command templates.

{ "templates": [ { "id": 2, "name": "Match IP", "field\_type": "IP", "description": null, "config\_specs": [ { "name": "ip", "type": "string", "subtype": "ip", "display\_name": "IP address", "description": "Enter the IP to compare with." } ], "query": "search $field$ == ip($ip$)", "query2": "search $field$ != ip($ip$)" }, { "id": 3, "name": "Match subnet", "field\_type": "IP", "description": null, "config\_specs": [ { "name": "subnet", "type": "string", "subtype": "subnet", "display\_name": "Subnet", "description": "Select a subnet to compare." } ], "query": "matchnet field=$field$ guid=$subnet$ verify=f", "query2": "matchnet invert=t field=$field$ guid=$subnet$ verify=f" } ]}

* **templates** (Array): List of all stream rule command templates
* **id** (32-bit integer): Template ID
* **name** (String): Template name
* **field\_type** (String): Applicable field type. One of the following: DATE, IP, PORT, STRING, SHORT, INT, LONG, MD5, URL.
* **description** (String): Template description
* **config\_specs** (Array): Template variable specification
* **name** (String): Variable name
* **type** (String): Variable type. One of the following: string, number, array.
* **subtype** (String): UI rendering hint, such as ip, date, country, port\_group. To support component selection with autocomplete and validation.
* **display\_name** (String): Display name in locale language
* **description** (String): Description in locale language
* **query** (String): Query string to be applied in the AND condition
* **query2** (String): Query string to be applied in the NOT condition

### Get Stream Rule Command Template

Retrieves information of a specified stream rule command template.

The stream rule command template is to support GUI-style editing of stream rules.

#### HTTP Request

GET /api/sonar/stream-rule-command-templates/:id

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/stream-rule-command-templates/2

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| id | O | 32-bit integer | Template ID |  |

#### Success Response

{ "template": { "id": 2, "name": "Match IP", "field\_type": "IP", "description": null, "config\_specs": [ { "name": "ip", "type": "string", "subtype": "ip", "display\_name": "IP address", "description": "Enter the IP to compare with." } ], "query": "search $field$ == ip($ip$)", "query2": "search $field$ != ip($ip$)" }}

* **template** (Map): Stream rule command template
* **id** (32-bit integer): Template ID
* **name** (String): Template name
* **field\_type** (String): Applicable field type. One of the following: DATE, IP, PORT, STRING, SHORT, INT, LONG, MD5, URL.
* **description** (String): Template description
* **config\_specs** (Array): Template variable specification
* **name** (String): Variable name
* **type** (String): Variable type. One of the following: string, number, array.
* **subtype** (String): UI rendering hint, such asip, date, country, port\_group. To support component selection with autocomplete and validation.
* **display\_name** (String): Display name in locale language
* **description** (String): Description in locale language
* **query** (String): Query string to be applied in the AND condition
* **query2** (String): Query string to be applied in the NOT condition

#### Error Response

id is not an integer

{ "error\_code": "invalid-argument", "error\_msg": "'id' parameter should be int type"}

## Batch Rule API

### Get Batch Rules

Gets a list of batch rules that match the specified search keyword.

#### HTTP Request

GET /api/sonar/batch-rules

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/batch-rules

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load | If not specified, load all records |
| keywords | X | String | Keywords | Search available by name, description, query target |

#### Success Response

Below is a partial list of batch rules.

{ "total\_count": 1, "rules": [ { "guid": "f4ca02c8-0679-49e7-8c10-76667c26b595", "priority": "LOW", "name": "DMZ 포트 스캔", "description": "", "msg": "DMZ 포트 스캔: $src\_ip", "enabled": false, "category\_guid": "8270a382-a47c-401d-9318-037c5d639f2e", "category\_name": "정보 수집", "schedule": "\*/10 \* \* \* \*", "duration": null, "datetrunc": null, "dataset\_guid": null, "dataset\_name": null, "query": "table duration=30m FW\_\*\n| fields \_time, \_schema, src\_ip, src\_port, dst\_ip, dst\_port, protocol, app, action, sent\_pkts, rcvd\_pkts, sent\_bytes, rcvd\_bytes\n| search \_schema == \"session\" and protocol == \"TCP\" and sent\_bytes <= 200\n| lookup geoip src\_ip output country as src\_country\n| lookup geoip dst\_ip output country as dst\_country\n| search src\_country != \"--\"\n| eval \_time = datetrunc(\_time, \"10m\") \n| stats dc(dst\_port) as port\_count, values(dst\_port) as dst\_port by src\_ip, dst\_ip, \_time \n| search port\_count >= 10 \n| explode dst\_port \n| eval protocol = \"TCP\" \n| order \_time, host\_count, src\_ip, dst\_ip, dst\_port, protocol", "address\_group\_guid": null, "address\_field": null, "ticket\_repo\_guid": null, "ticket\_assignee\_guid": null, "ticket\_assignee\_name": null, "ticket\_suppress\_interval": 3600, "event\_suppress\_interval": 0, "suppress\_key": null, "keep\_alive": false, "audit\_category\_guid": null, "audit\_category\_name": null, "auditor\_guid": null, "auditor\_name": null, "audit\_days": 14, "employee\_key\_field": null, "alarm\_group\_guid": null, "alarm\_group\_name": null, "field\_order": "\_time, host\_count, src\_ip, dst\_ip, dst\_port, protocol", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": null, "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "관리자", "created": "2022-09-01 00:31:15+0900", "updated": "2022-09-01 00:31:15+0900" } ]}

* **total\_count** (32-bit integer): Total number of the batch rules that match the search keyword.
* **rules** (Array): Paged list of batch rules
* **priority** (String): LOW or MEDIUM or HIGH
* **guid** (String): Batch Rule GUID
* **name** (String): Batch Rule name
* **description** (String): Batch rule description
* **msg** (String): Message template. Macro in the $field format available.
* **enabled** (Boolean): Whether the rule is enabled or not
* **category\_guid** (String): Batch rule category GUID
* **category\_name** (String): Batch rule category name
* **schedule** (String): Execution schedule in CRON schedule format
* **duration** (32-bit integer): Time window of the data to be analyzed, based on the current time (in seconds). The value is passed to the from and to parameters of the query.
* **datetrunc** (32-bit integer): Date truncation unit (in seconds). Date truncation unit for the from, to parameters of the query.
* **dataset\_guid** (String): Dataset GUID
* **dataset\_name** (String): Dataset name
* **address\_group\_guid** (String): Address group GUID
* **address\_field** (String): Target fields to add to the address group
* **ticket\_repo\_guid** (String): Ticket repository GUID
* **ticket\_assignee\_guid** (String): Ticket assignee GUID
* **ticket\_assignee\_name** (String): Ticket assignee name
* **ticket\_suppress\_interval** (32-bit integer): Suppression period for duplicated ticket in seconds (in seconds)
* **event\_suppress\_interval** (32-bit integer): Suppression period for duplicated event in seconds (in seconds)
* **suppress\_key** (String): Suppress key field. Macro in the $field format available.
* **keep\_alive** (Boolean): true to keep the timer alive, false to reset it.
* When keeping the suppression timer, even if a user completes the ticket, the event will be merged into the existing ticket until the expiration time is reached.
* **audit\_category\_guid** (String): Audit category GUID
* **audit\_category\_name** (String): Audit category name
* **auditor\_guid** (String): Auditor GUID. If not specified, the department head is assigned as default.
* **auditor\_name** (String): Auditor name. If not specified, the department head is assigned as default.
* **audit\_days** (32-bit integer): Audit due date (days)
* **employee\_key\_field** (String): Employee number field. Typically using a normalized emp\_key field.
* **alarm\_group\_guid** (String): Alarm group GUID
* **alarm\_group\_name** (String): Alarm group name
* **field\_order** (String): Evidence file output order. Comma-separated list of field names.
* **company\_guid** (String): GUID of the company (tenant) to which the batch rule belongs
* **company\_name** (String): Name of the company (tenant) to which the batch rule belongs
* **user\_guid** (String): GUID of the user who creates the batch rule
* **user\_name** (String): Name of the user who creates the batch rule
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

### Get Batch Rule

Gets a specified batch rule.

#### HTTP Request

GET /api/sonar/batch-rules/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/batch-rules/f4ca02c8-0679-49e7-8c10-76667c26b595

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Batch rule GUID | 36 characters |

#### Success Response

Below is a partial list of batch rules.

{ "rule": { "guid": "f4ca02c8-0679-49e7-8c10-76667c26b595", "priority": "LOW", "name": "DMZ 포트 스캔", "description": "", "msg": "DMZ 포트 스캔: $src\_ip", "enabled": false, "category\_guid": "8270a382-a47c-401d-9318-037c5d639f2e", "category\_name": "정보 수집", "schedule": "\*/10 \* \* \* \*", "duration": null, "datetrunc": null, "dataset\_guid": null, "dataset\_name": null, "query": "table duration=30m FW\_\*\n| fields \_time, \_schema, src\_ip, src\_port, dst\_ip, dst\_port, protocol, app, action, sent\_pkts, rcvd\_pkts, sent\_bytes, rcvd\_bytes\n| search \_schema == \"session\" and protocol == \"TCP\" and sent\_bytes <= 200\n| lookup geoip src\_ip output country as src\_country\n| lookup geoip dst\_ip output country as dst\_country\n| search src\_country != \"--\"\n| eval \_time = datetrunc(\_time, \"10m\") \n| stats dc(dst\_port) as port\_count, values(dst\_port) as dst\_port by src\_ip, dst\_ip, \_time \n| search port\_count >= 10 \n| explode dst\_port \n| eval protocol = \"TCP\" \n| order \_time, host\_count, src\_ip, dst\_ip, dst\_port, protocol", "address\_group\_guid": null, "address\_field": null, "ticket\_repo\_guid": null, "ticket\_assignee\_guid": null, "ticket\_assignee\_name": null, "ticket\_suppress\_interval": 3600, "event\_suppress\_interval": 0, "suppress\_key": null, "keep\_alive": false, "audit\_category\_guid": null, "audit\_category\_name": null, "auditor\_guid": null, "auditor\_name": null, "audit\_days": 14, "employee\_key\_field": null, "alarm\_group\_guid": null, "alarm\_group\_name": null, "field\_order": "\_time, host\_count, src\_ip, dst\_ip, dst\_port, protocol", "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "로그프레소", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "관리자", "created": "2022-09-01 00:31:15+0900", "updated": "2022-09-01 00:31:15+0900" }}

* **rule** (Map): Batch rule
* **priority** (String): LOW, MEDIUM, HIGH
* **guid** (String): Batch rule GUID
* **name** (String): Batch rule name
* **description** (String): Batch rule description
* **msg** (String): Message template. Macro in the $field format available.
* **enabled** (Boolean): Whether the rule is enabled or not
* **category\_guid** (String): Batch rule category GUID
* **category\_name** (String): Batch rule category name
* **schedule** (String): Execution schedule in CRON schedule format
* **duration** (32-bit integer): Time window of the data to be analyzed, based on the current time (in seconds). The value is passed to the from and to parameters of the query.
* **datetrunc** (32-bit integer): Date truncation unit (in seconds). Date truncation unit for the from, to parameters of the query.
* **dataset\_guid** (String): Dataset GUID
* **dataset\_name** (String): Dataset name
* **address\_group\_guid** (String): Address group GUID
* **address\_field** (String): Target field to add to the address group
* **ticket\_repo\_guid** (String): Ticket repository GUID
* **ticket\_assignee\_guid** (String): Ticket assignee GUID
* **ticket\_assignee\_name** (String): Ticket assignee name
* **ticket\_suppress\_interval** (32-bit integer): Suppression period for duplicated ticket in seconds (in seconds)
* **event\_suppress\_interval** (32-bit integer): Suppression period for duplicated event in seconds (in seconds)
* **suppress\_key** (String): Suppress key field. Macro in the $field format available.
* **keep\_alive** (Boolean): true to keep the timer alive, false to reset it.
* When keeping the suppression timer, even if a user completes the ticket, the event will be merged into the existing ticket until the expiration time is reached.
* **audit\_category\_guid** (String): Audit category GUID
* **audit\_category\_name** (String): Audit category name
* **auditor\_guid** (String): Auditor GUID. If not specified, the department head is assigned as default.
* **auditor\_name** (String): Auditor name. If not specified, the department head is assigned as default.
* **audit\_days** (32-bit integer): Audit due date (days)
* **employee\_key\_field** (String): Employee number field. Typically using a normalized emp\_key field.
* **alarm\_group\_guid** (String): Alarm group GUID
* **alarm\_group\_name** (String): Alarm group name
* **field\_order** (String): Evidence file output order. Comma-separated list of field names.
* **company\_guid** (String): GUID of the company (tenant) to which the batch rule belongs
* **company\_name** (String): Name of the company (tenant) to which the batch rule belongs
* **user\_guid** (String): GUID of the user who creates the batch rule
* **user\_name** (String): Name of the user who creates the batch rule
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

#### Error Responses

Batch rule is not found

HTTP status code 200

{ "rule": null}

Identifier is not in valid GUID format

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

### Create Batch Rule

Creates a new batch rule.

#### HTTP Request

POST /api/sonar/batch-rules

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d priority="LOW" \ -d name="Scan web vulnerabilities" \ -d schedule="\*/30 \* \* \* \*" -d msg="Scan web vulnerabilities: $dst\_ip" \ -d query="table duration=30m weblog | search status >= 400 | stats count as error\_count, dc(path) as page\_count, values(concat(method, " ", path)) as request by src\_ip | eval request = strjoin("\n", request) | lof eps=0.1 error\_count, page\_count | search \_lof > 1.5 | sort -\_lof" \ -X POST \ https://HOSTNAME/api/sonar/batch-rules

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| priority | O | String | Priority | LOW or MEDIUM or HIGH |
| guid | X | String | Batch rule GUID | 36 characters |
| name | O | String | Batch rule name | Minimum 1 to maximum 255 characters |
| description | X | String | Batch rule description | Maximum 2,000 characters |
| msg | O | String | Message template | Minimum 1 to maximum 2,000 characters |
| enabled | X | Boolean | Whether the batch rule is enabled | true or false |
| category\_guid | X | String | Batch rule category GUID | 36 characters |
| schedule | O | String | Execution cycle | CRON schedule format |
| duration | X | 32-bit integer | Time window of the data to be analyzed, based on the current time | Up to 31536000 seconds (365 days) |
| datetrunc | X | 32-bit integer | Date truncation unit | 1 or 60 or 3600 or 86400 (seconds) |
| dataset\_guid | X | String | Dataset GUID | 36 character. At least one of dataset\_guid and query must be provided. |
| query | X | String | Detection query | Maximum 65,535 characters. At least one of dataset\_guid and query must be provided. |
| address\_group\_guid | X | String | Address group GUID | 36 characters |
| address\_field | X | String | Address field name | Address group field name. Maximum 50 characters. |
| ticket\_repo\_guid | X | String | Ticket repository GUID | 36 characters. If not specified, a ticket is not generated. |
| ticket\_assignee\_guid | X | String | Ticket assignee GUID | If specified, a ticket is assigned automatically. |
| ticket\_suppress\_interval | X | 32-bit integer | Suppression period for duplicate ticket (in seconds) | If set to 0 or not specified, duplicate tickets are not merged. |
| event\_suppress\_interval | X | 32-bit integer | Suppression period for duplicated event (in seconds) | If set to 0 or not specified, duplicate events are not merged. |
| suppress\_key | X | String | Suppress key field | Maximum 2,000 characters. Macro in $field format available. |
| keep\_alive | X | Boolean | Whether to keep the suppression timer alive | true to keep the timer alive, false to reset it. |
| audit\_category\_guid | X | String | Audit category GUID | 36 characters. If not specified, an auto audit request is not sent. |
| auditor\_guid | X | String | Auditor GUID | 36 characters. If not specified, the department head is assigned as default. |
| audit\_days | X | 32-bit integer | Audit due date | Minimum 1 to maximum 365 days |
| employee\_key\_field | X | String | Employee number field | Maximum 50 characters. If not specified, an auto audit request is not sent. |
| alarm\_group\_guid | X | String | Alarm group GUID | 36 characters |
| field\_order | X | String | Evidence field output order | Maximum 2,000 characters |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "schedule should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'address\_field' must be shorter than or equal to 50 characters."}

Invalid priority value

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "priority should be one of 'LOW', 'MEDIUM', 'HIGH'."}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "category\_guid should be guid type."}

CRON expression is not valid

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "schedule has wrong cron expression format: \* \* \* \* \* \*"}

Both dataset and query are not specified

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "query should be not null"}

Invalid date truncation unit value

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "datetrunc should be one of 1 (1 second), 60 (1 minute), 3600 (1 hour), 86400 (1 day)."}

No privilege to create a batch rule

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Update Batch Rule

Updates a specified batch rule.

#### HTTP Request

PUT /api/sonar/batch-rules/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d priority="LOW" \ -d name="Scan web vulnerabilities" \ -d schedule="\*/10 \* \* \* \*" -d msg="Scan web vulnerabilities: $dst\_ip" \ -d query="table duration=30m weblog | search status >= 400 | stats count as error\_count, dc(path) as page\_count, values(concat(method, " ", path)) as request by src\_ip | eval request = strjoin("\n", request) | lof eps=0.1 error\_count, page\_count | search \_lof > 1.5 | sort -\_lof" \ -X PUT \ https://HOSTNAME/api/sonar/batch-rules/410fe6af-b2f8-4674-af70-8d5b12ddc3fe

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| priority | O | String | Priority | LOW, MEDIUM, HIGH |
| guid | O | String | Batch rule GUID | 36 characters |
| name | O | String | Batch rule name | Minimum 1 to maximum 255 characters |
| description | X | String | Batch rule description | Maximum 2,000 characters |
| msg | O | String | Message template | Minimum 1 to maximum 2,000 characters |
| enabled | X | Boolean | Whether the rule is enabled or not | true or false |
| category\_guid | X | String | Batch rule category GUID | 36 characters |
| schedule | O | String | Execution schedule | In CRON schedule format |
| duration | X | 32-bit integer | Time window of the data to be analyzed, based on the current time | In seconds. Maximum 31536000 second (365 days) |
| datetrunc | X | 32-bit integer | Time truncation | 1 or 60 or 3600 or 86400 (seconds) |
| dataset\_guid | X | String | Dataset GUID | At least one of dataset\_guid and query must be provided. 36 characters long |
| query | X | String | Detection query | Maximum 65,535 characters. At least one of dataset\_guid and query must be provided. |
| address\_group\_guid | X | String | Address group GUID | 36 characters |
| address\_field | X | String | Address field | Address group field name. Maximum 50 characters. |
| ticket\_repo\_guid | X | String | Ticket repository GUID | 36 characters. If not specified, a ticket is not generated. |
| ticket\_assignee\_guid | X | String | Ticket assignee GUID | If specified, ticket is assigned automatically |
| ticket\_suppress\_interval | X | 32-bit integer | Suppression period for duplicated ticket in seconds | If set to 0 or not specified, duplicate tickets are not merged. |
| event\_suppress\_interval | X | 32-bit integer | Suppression period for duplicated event in seconds | If set to 0 or not specified, duplicate events are not merged. |
| suppress\_key | X | String | Suppress key field | Maximum 2,000 characters. Macro in $field format available. |
| keep\_alive | X | Boolean | Whether to keep the suppression timer alive | true to keep the timer alive, false to reset it. |
| audit\_category\_guid | X | String | Audit category GUID | If not specified, an auto audit request is not sent. 36 characters long |
| auditor\_guid | X | String | Auditor GUID | 36 characters. If not specified, the department head is assigned as default. |
| audit\_days | X | 32-bit integer | Audit due date | Minimum 1 to maximum 365 days |
| employee\_key\_field | X | String | Employee number field | Maximum 50 characters. If not specified, an auto audit request is not sent. |
| alarm\_group\_guid | X | String | Alarm group GUID | 36 characters |
| field\_order | X | String | Evidence field output order | Maximum 2,000 characters |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "schedule should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'address\_field' must be shorter than or equal to 50 characters."}

Invalid priority value

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "priority should be one of 'LOW', 'MEDIUM', 'HIGH'."}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "category\_guid should be guid type."}

CRON expression is not valid

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "schedule has wrong cron expression format: \* \* \* \* \* \*"}

Both dataset and query are not specified

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "query should be not null"}

Invalid value for `datetrunc`

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "datetrunc should be one of 1 (1 second), 60 (1 minute), 3600 (1 hour), 86400 (1 day)."}

Batch rule is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "batch rule not found: 9071a6fe-6b91-4448-9761-7123381cb026"}

No privilege to create a batch rule

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Remove Batch Rules

Deletes the specified batch rules.

#### HTTP Request

DELETE /api/sonar/batch-rules

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/batch-rules?guids=638cfeb2-e259-46af-961a-1eeb65ea35f0"

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guids | O | List (of strings) | Batch rule GUID list | Comma-separated list |

#### Success Response

{ "failures": []}

#### Error Responses

Batch rule is not found

HTTP status code 200

{ "failures": [ { "id": "638cfeb2-e259-46af-961a-1eeb65ea35f1", "reason": "batch-rule-not-found" } ]}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

### Run Batch Rule

Runs a specified batch rule immediately. The system runs the batch rule query asynchronously, so it responds without waiting for the query to complete. Execution does not raise an event or ticket in the following cases:

* The batch rule is disabled.
* The batch rule is deleted during query execution.

#### HTTP Request

POST /api/sonar/batch-rules/:guid/run

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/batch-rules/c4ca4744-f310-4480-baa8-0548067abfb3/run

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Batch rule GUID | 36 characters |

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Batch rule is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "batch rule not found: 05efb651-9644-4518-950f-dbd648c973a7"}

### Enable Batch Rule

Enables a specified batch rule.

#### HTTP Request

POST /api/sonar/batch-rules/:guid/enable

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/batch-rules/c4ca4744-f310-4480-baa8-0548067abfb3/enable

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Batch rule GUID | 36 characters |

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Batch rule is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "batch rule not found: 05efb651-9644-4518-950f-dbd648c973a7"}

Batch rule is already enabled

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "batch rule is already enabled: c4ca4744-f310-4480-baa8-0548067abfb3""}

No privileges to enable a batch rule

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Disable Batch Rule

Disables a specified batch rule.

#### HTTP Request

POST /api/sonar/batch-rules/:guid/disable

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/batch-rules/c4ca4744-f310-4480-baa8-0548067abfb3/disable

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Batch rule GUID | 36 characters |

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Batch rule is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "batch rule not found: 05efb651-9644-4518-950f-dbd648c973a7"}

Batch rule is already disabled

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "batch rule is already disabled: c4ca4744-f310-4480-baa8-0548067abfb3""}

No privileges to enable a batch rule

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## Ticket API

### Get Tickets

Gets a list of the tickets that match the search keyword.

#### HTTP Request

GET /api/sonar/tickets

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/tickets

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load | Minimum 0 to maximum 1000. If not specified, 1000 |
| from | X | Date | Start date | yyyy-MM-dd HH:mm:ssZ format. The start date is included in the range. |
| to | X | Date | End date | yyyy-MM-dd HH:mm:ssZ format. The end date is included in the range. |
| statuses | X | List (of strings) | Status | Comma-separated list. Refer to the below status codes. |
| keywords | X | String | Keyword |  |
| priorities | X | List (of 32-bit integers) | Priority list | High (3), Medium (2), Low (1). Comma-sepated list |
| assignees | X | List (of strings) | List of assignees | Comma-separated user GUID list |
| approvers | X | List (of strings) | List of approvers | Comma-separated user GUID list |
| sort\_type | X | String | Sorting type | ASCor DESC |
| sort\_column | X | String | Sorting key | id or created\_at or updated\_at or closed\_at |

Ticket status code

* New (NEW)
* Assigned (ASSIGNED)
* In process (IN\_PROGRESS)
* Submitted (SUBMITTED)
* Approved (APPROVED)
* Rejected (REJECTED)
* Closed (CLOSED)

#### Success Response

{ "total": 15, "tickets": [ { "id": 2, "repo\_guid": "5f0ba741-7551-400d-8bd6-1f14a6e8536d", "repo\_name": "Threat", "guid": "49272877-75f2-4c2f-9301-d21c4f9a106d", "title": "Attempt to collect web server settings: 20.0.31.172", "priority": "LOW", "status": "ASSIGNED", "format": "JSON", "count": 7, "attack": true, "incident": false, "assignees": [ { "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "user\_guid": "bfd00bb0-be99-4fd5-8380-166f544975fa", "user\_name": "Joshua", "task\_type": "ASSIGNEE", "task\_status": "ASSIGNED", "x\_login": null, "x\_user": null, "x\_dept": null } ], "approvers": [], "created": "2022-09-14 17:34:19+0900", "updated": "2022-09-14 23:55:29+0900", "closed": null, "x\_login": null, "x\_user": null, "x\_dept": null } ]}

* (32-bit integer) total
* (Array) tickets
* **id** (32-bit integer): Ticket ID
* **repo\_guid** (String): Ticket type GUID
* **repo\_name** (String): Ticket type name
* **site\_guid** (String): Site GUID
* **site\_name** (String): Site name
* **guid** (String): Ticket GUID
* **title** (String): Title
* **priority** (String): Ticket priority. One of the following: HIGH, MEDIUM, LOW.
* **status** (String): Ticket status. One of the following: NEW, ASSIGNED, IN\_PROGRESS, SUBMITTED, APPROVED, REJECTED, CLOSED.
* **format** (String): Ticket format. One of the following: JSON, MARKDOWN, PLAIN. Threat detection ticket uses JSON format.
* **count** (32-bit integer): Number of merged duplicate ticket
* **attack** (Boolean): Whether the detection is false or not, recorded after analysis. Logged as true if the detection is true.
* **incident** (Boolean): Whether an incident occurred or not, recorded after analysis. Recorded as true if the incident requires an immediate response, such as an endpoint infection.
* **assignees** (Array): Ticket assignee list
* **company\_guid** (String): Company (tenant) GUID
* **company\_name** (String): Company (tenant) name
* **user\_guid** (String): Assignee identifier
* **user\_name** (String): Assignee GUID
* **task\_type** (String): Always ASSIGNEE
* **task\_status** (String): ASSIGNED or IN\_PROGRESS or CLOSED
* **x\_login** (String): Login user name logged when logged when the assignee account is deleted
* **x\_user** (String): User name logged when logged when the assignee account is deleted
* **x\_dept** (String): Department name logged when logged when the assignee account is deleted
* **approvers** (Array): List of ticker approvers
* **company\_guid** (String): Company (tenant) GUID
* **company\_name** (String): Company (tenant) name
* **user\_guid** (String): Approver GUID
* **user\_name** (String): Approver name
* **task\_type** (String): Always APPROVER
* **task\_status** (String): ASSIGNED or IN\_PROGRESS or CLOSED
* **x\_login** (String): Login user name logged when logged when the approver account is deleted
* **x\_user** (String): User name logged when logged when the approver account is deleted
* **x\_dept** (String): Department name logged when logged when the approver account is deleted
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)
* **closed** (String): Date and time of ticket closing (yyyy-MM-dd HH:mm:ssZ)
* **x\_login** (String): Login user name logged when logged when the ticket author account is deleted
* **x\_user** (String): User name logged when logged when the ticket author account is deleted
* **x\_dept** (String): Department name logged when logged when the ticket author account is deleted
* **x\_site** (String): Site name logged when logged when the site is deleted

#### Error Responses

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' parameter should be int type"}

offset or limit value is negative

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

Invalid `from`, `to` date formats

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'from' parameter should be date format (yyyy-MM-dd HH:mm:ss+0000)"}

Undefined status code

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'statuses' should contain elements that is one of NEW, ASSIGNED, IN\_PROGRESS, SUBMITTED, APPROVED, REJECTED, CLOSED."}

Undefined priority value

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "element of priorities should be one of 1 (LOW), 2 (MEDIUM), 3 (HIGH). input is 4"}

Undefined sorting type

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "sort\_type should be one of ASC or DESC. input is NONE"}

Invalid sorting key column

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "sort\_column should be one of id, created\_at, updated\_at, closed\_at."}

List of assignees or approvers has non-GUID value

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "assignees should contains only guid values."}

### Get Ticket

Retrieves information of a specified ticket.

#### HTTP Request

GET /api/sonar/tickets/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/tickets/49272877-75f2-4c2f-9301-d21c4f9a106d

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Ticket GUID | 36 characters |

#### Success Response

{ "ticket": { "id": 2, "repo\_guid": "5f0ba741-7551-400d-8bd6-1f14a6e8536d", "repo\_name": "Threat", "guid": "49272877-75f2-4c2f-9301-d21c4f9a106d", "title": "Attempt to collect web server settings: 20.0.31.172", "priority": "LOW", "status": "APPROVED", "format": "JSON", "rule\_guid": "ad4b9871-d5f0-4a8b-a341-8ac0afcdcddf", "rule\_type": "STREAM", "rule\_name": "Attempt to collect web server settings", "count": 7, "content": "{\"first\_seen\":\"2022-09-14 17:34:19+0900\",\"last\_seen\":\"2022-09-14 23:55:29+0900\",\"priority\":\"LOW\",\"rule\_type\":\"STREAM\",\"rule\_id\":27,\"src\_ip\":\"20.0.31.172\",\"src\_port\":null,\"dst\_ip\":null,\"dst\_port\":null,\"protocol\":null,\"action\":null,\"count\":1,\"msg\":\"웹 서버 설정 수집 시도: 20.0.31.172\",\"user\":null,\"host\_ip\":null,\"mail\_from\":null,\"mail\_to\":null,\"mail\_cc\":null,\"logger\_id\":28,\"logger\_name\":\"ko.logpresso.com \",\"field\_order\":\"\_time, src\_ip, src\_port, dst\_ip, dst\_port, status, method, path, query, user\_agent\",\"url\":null,\"md5\":null,\"src\_asn\":\"AS8075 Microsoft Corporation\",\"src\_country\":\"US\",\"src\_city\":null,\"src\_lat\":37.750999450683594,\"src\_lng\":-97.8219985961914}", "attack": true, "incident": false, "assignees": [ { "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "user\_guid": "bfd00bb0-be99-4fd5-8380-166f544975fa", "user\_name": "Joshua", "task\_type": "ASSIGNEE", "task\_status": "CLOSED", "x\_login": null, "x\_user": null, "x\_dept": null } ], "approvers": [ { "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "Jerry", "task\_type": "APPROVER", "task\_status": "APPROVED", "x\_login": null, "x\_user": null, "x\_dept": null } ], "attachments": [ { "guid": "d4390b7a-7d64-4a24-bd3e-af74b4f3c204", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "ticket\_guid": "49272877-75f2-4c2f-9301-d21c4f9a106d", "file\_name": "3bc31b3d-bc25-4be5-8dae-d3cb1831da02.png", "file\_size": 124118 } ], "created": "2022-09-14 17:34:19+0900", "updated": "2022-09-14 23:55:29+0900", "closed": null, "x\_login": null, "x\_user": null, "x\_dept": null, "comments": [ { "guid": "b66a31b5-db94-478b-8751-194b5ee5f358", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "Joshua", "type": "TEXT", "format": "MARKDOWN", "content": "\* Blocked the IP address in firewall.", "created": "2022-09-14 23:57:34+0900", "updated": "2022-09-14 23:57:34+0900", "x\_login": null, "x\_user": null, "x\_dept": null } ] }}

* (Map) ticket
* **id** (32-bit integer): Ticket ID
* **repo\_guid** (String): Ticket type GUID
* **repo\_name** (String): Ticket type name
* **site\_guid** (String): Site GUID
* **site\_name** (String): Site name
* **guid** (String): Ticket GUID
* **title** (String): Ticket title
* **priority** (String): Ticket priority. One of the following: HIGH, MEDIUM, LOW.
* **status** (String): Ticket status. One of the following: NEW, ASSIGNED, IN\_PROGRESS, SUBMITTED, APPROVED, REJECTED, CLOSED.
* **format** (String): Ticket format. One of the following: JSON, MARKDOWN, PLAIN. Threat detection ticket uses JSON format.
* **rule\_guid** (String): Detection rule GUID
* **rule\_type** (String): Detection rule type. STREAM or BATCH.
* **rule\_name** (String): Detection rule name
* **count** (32-bit integer): Number of merged duplicate tickets
* **content** (String): Ticket data. The Event field is written in JSON format for threat detection tickets.
* **attack** (Boolean): Whether the detection is false or not, recorded after analysis. Logged as true if the detection is true
* **incident** (Boolean): Whether an incident occurred or not, recorded after analysis. Recorded as true if the incident requires an immediate response, such as an endpoint infection.
* **assignees** (Array): Ticket assignee list
* **company\_guid** (String): Company (tenant) GUID
* **company\_name** (String): Company (tenant) name
* **user\_guid** (String): Assignee GUID
* **user\_name** (String): Assignee name
* **task\_type** (String): Always ASSIGNEE
* **task\_status** (String): ASSIGNED or IN\_PROGRESS or CLOSED
* **x\_login** (String): Login user name logged when the assignee account is deleted
* **x\_user** (String): User name logged when the assignee account is deleted
* **x\_dept** (String): Department name logged when the assignee account is deleted
* **approvers** (Array): Ticket approver list
* **company\_guid** (String): Company (tenant) GUID
* **company\_name** (String): Company (tenant) name
* **user\_guid** (String): Approver GUID
* **user\_name** (String): Approver name
* **task\_type** (String): Always APPROVER
* **task\_status** (String): ASSIGNED or IN\_PROGRESS or CLOSED
* **x\_login** (String): Login user name logged when the approver account is deleted
* **x\_user** (String): User name logged when the approver account is deleted
* **x\_dept** (String): Department name logged when the approver account is deleted
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)
* **closed** (String): Date and time of ticket closing (yyyy-MM-dd HH:mm:ssZ)
* **x\_login** (String): Login user name logged when the ticket author account is deleted
* **x\_user** (String): User name logged when the ticket author account is deleted
* **x\_dept** (String): Department name logged when the ticket author account is deleted
* **x\_site** (String): Site name logged when the site is deleted
* **comments** (Array): Ticket comment list
* **guid** (String): Ticket comment GUID
* **user\_guid** (String): Ticket author GUID
* **user\_name** (String): Ticket author name
* **type** (String): Always TEXT
* **format** (String): Markdown (MARKDOWN) or plain text (PLAIN)
* **content** (String): Comment content
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)
* **x\_login** (String): Login user name logged when logged when the ticket comment author account is deleted
* **x\_user** (String): User name logged when logged when the ticket comment author account is deleted
* **x\_dept** (String): Department name logged when logged when the ticket comment author account is deleted

#### Error Responses

Ticket is not found

HTTP status code 200

{ "ticket": null}

Ticket identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

### Create Ticket

Creates a new ticket.

#### HTTP Request

POST /api/sonar/tickets

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d repo\_guid=5f0ba741-7551-400d-8bd6-1f14a6e8536d \ -d guid=638cfeb2-e259-46af-961a-1eeb65ea35f0 \ -d priority=LOW \ -d title="Attempt to collect web server settings" \ -d format=JSON \ --data-urlencode content="{""first\_seen"":""2022-09-20 14:55:54+0900"",""last\_seen"":""2022-09-20 14:55:54+0900"",""priority"":""LOW"",""src\_ip"":""3.83.23.230"",""dst\_ip"":""13.125.82.152"",""dst\_port"":443}" \ -X POST \ https://HOSTNAME/api/sonar/tickets

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| repo\_guid | O | String | Ticket repository GUID | 36 characters |
| guid | O | String | Ticket GUID | 36 characters |
| priority | O | String | Priority | LOW or MEDIUM or HIGH |
| title | O | String | Title | Minimum 1 to maximum 255 characters |
| format | O | String | Content format | JSON or MARKDOWN or PLAIN |
| content | O | String | Content | Minimum 1 to maximum 100,000 characters |
| assignees | X | List (of strings) | Assignee GUID list | Comma-separated list |
| approvers | X | List (of strings) | Approver GUID list | Comma-separated list |
| attachments | X | List (of strings) | Attachment GUID list | Comma-separated list |

Attachments refer to file objects that have already been uploaded, so they can exist before the ticket is created. Unreferenced ticket file objects are automatically destroyed at midnight each day.

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "repo\_guid should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'title' must be shorter than or equal to 255 characters."}

Invalid priority value

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "priority should be one of 'LOW', 'MEDIUM', 'HIGH'."}

Invalid format specified

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "format should be one of 'JSON', 'MARKDOWN', 'PLAIN'."}

Content is not in JSON format

When the content format(format) is specified as JSON, an error occurs if the content is not in JSON format.

{ "error\_code": "invalid-argument", "error\_msg": "content should be JSON format - Expected a ',' or '}' at character 146"}

List of assignees or approvers has non-GUID value

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "assignees should be guid type."}

Duplicate ticket GUID is found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "duplicated ticket guid: 638cfeb2-e259-46af-961a-1eeb65ea35f0"}

Assignee or approver is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "assignee not found: fae7fa2b-756e-4d3d-b314-e631daf70c7a"}

Attachment is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "attachment not found: 8e904789-b9b9-443a-b1a1-86a36119c74c"}

### Update Ticket

Updates a specified ticket.

#### HTTP Request

PUT /api/sonar/tickets/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d priority=HIGH \ -d title="Attempt to collect web server settings" \ -d format=JSON \ --data-urlencode content="{""first\_seen"":""2022-09-20 14:55:54+0900"",""last\_seen"":""2022-09-20 19:44:24+0900"",""priority"":""HIGH"",""src\_ip"":""3.83.23.230"",""dst\_ip"":""13.125.82.152"",""dst\_port"":443}" \ -X PUT \ https://HOSTNAME/api/sonar/tickets/638cfeb2-e259-46af-961a-1eeb65ea35f0

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Ticket GUID | 36 characters |
| priority | O | String | Priority | LOW or MEDIUM or HIGH |
| title | O | String | Title | Minimum 1 to maximum 255 characters |
| format | O | String | Content format | JSON or MARKDOWN or PLAIN |
| content | O | String | Content | Minimum 1 to maximum 100,000 characters |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "title should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'title' must be shorter than or equal to 255 characters."}

Invalid `Priority` value

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "priority should be one of 'LOW', 'MEDIUM', 'HIGH'."}

Invalid format is specified

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "format should be one of 'JSON', 'MARKDOWN', 'PLAIN'."}

Content is not in JSON format

When the content format (format) is specified as JSON, an error occurs if content (content) is not in JSON format.

{ "error\_code": "invalid-argument", "error\_msg": "content should be JSON format - Expected a ',' or '}' at character 146"}

Ticket is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 638cfeb2-e259-46af-961a-1eeb65ea35f1"}

Update a ticket generated by system

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "cannot update system ticket: 638cfeb2-e259-46af-961a-1eeb65ea35f1"}

### Remove Tickets

Deletes the specified tickets.

#### HTTP Request

DELETE /api/sonar/tickets

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ "https://HOSTNAME/api/sonar/tickets?guids=638cfeb2-e259-46af-961a-1eeb65ea35f0"

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guids | O | List (of strings) | Ticket GUID list | Comma-separated list |

#### Success Response

{ "failures": []}

#### Error Responses

Ticket is not found

HTTP status code 200

{ "failures": [ { "id": "638cfeb2-e259-46af-961a-1eeb65ea35f1", "reason": "ticket-not-found" } ]}

Ticket Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

### Update Ticket Priority

Updates the priority of a specified ticket.

#### HTTP Request

PUT /api/sonar/tickets/:guid/priority

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d priority=HIGH \ -X PUT \ https://HOSTNAME/api/sonar/tickets/201dc306-5ef7-4d4f-b872-1fa0f4d7dc56/priority

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Ticket GUID | 36 characters |
| priority | O | String | Priority | LOW or MEDIUM or HIGH |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "priority should be not null"}

Ticket identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Ticket is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

### Update Ticket Title

Updates the title of a specified ticket.

#### HTTP Request

PUT /api/sonar/tickets/:guid/title

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d title="Updated title" \ -X PUT \ https://HOSTNAME/api/sonar/tickets/201dc306-5ef7-4d4f-b872-1fa0f4d7dc56/title

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Ticket GUID | 36 characters |
| title | O | String | Ticket title | Minimum 1 to maximum 255 characters |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "title should be not null"}

Ticket identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'title' must be shorter than or equal to 255 characters."}

Ticket is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

### Update Ticket Attack

Updates the attack status of a specified ticket.

#### HTTP Request

PUT /api/sonar/tickets/:guid/attack

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d attack=true \ -X PUT \ https://HOSTNAME/api/sonar/tickets/201dc306-5ef7-4d4f-b872-1fa0f4d7dc56/attack

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Ticket GUID | 36 characters |
| attack | X | Boolean | Attack status | If not specified, null. |

#### Success Response

{}

#### Error Responses

Ticket identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Ticket is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

### Update Ticket Incident

Updates the incident status of a specified ticket.

#### HTTP Request

PUT /api/sonar/tickets/:guid/incident

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d incident=true \ -X PUT \ https://HOSTNAME/api/sonar/tickets/201dc306-5ef7-4d4f-b872-1fa0f4d7dc56/incident

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Ticket GUID | 36 characters |
| incident | X | Boolean | Incident status | If not specified, null. |

#### Success Response

{}

#### Error Responses

Ticket identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Ticket is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

### Assign Ticket

Assigns a ticket to the specified users.

#### HTTP Request

POST /api/sonar/tickets/:guid/assign

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d type=ASSIGNEE \ -d assignees=fae7fa2b-756e-4d3d-b314-e631daf70c7d \ -X POST \ https://HOSTNAME/api/sonar/tickets/6206eb0e-fb44-4f13-82ca-d92454cfd35e/assign

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Ticket GUID | 36 characters |
| type | O | String | Assigned role | ASSIGNEE or APPROVER |
| assignees | O | List (of strings) | User GUID list | Comma-separated list |

#### Success Response

{}

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Ticket is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

### Get Ticket Assignees

Gets a list of the assignees or approvers that are assigned to a specific ticket.

#### HTTP Request

GET /api/sonar/tickets/:guid/assignees

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ "https://HOSTNAME/api/sonar/tickets/c63ff706-85bc-44e3-9acd-24a0628da1fb/assignees?type=APPROVER"

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| type | O | String | Assigned role | ASSIGNEE or APPROVER |

#### Success Response

{ "assignees": [ { "company\_guid": "6fbe27b7-f1ae-4d7a-a1a5-76d8fa9aa311", "company\_name": "Logpresso", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "Joshua", "task\_type": "APPROVER", "task\_status": "APPROVED", "x\_login": null, "x\_user": null, "x\_dept": null } ]}

* **assignees** (Array): List of assignees or approvers
* **company\_guid** (String): Company (tenant) GUID
* **company\_name** (String): Company (tenant) name
* **user\_guid** (String): GUID of the assignee or approver
* **user\_name** (String): Name of the assignee or approver
* **task\_type** (String): ASSIGNEE or APPROVER
* **task\_status** (String): Ticket status
* For an assignee, one of the following: ASSIGNED, IN\_PROGRESS, CLOSED.
* For an approver, one of the following: ASSIGNED, ASSIGNED, REJECTED.
* **x\_login** (String): Login user name logged when the assignee/approver account is deleted
* **x\_user** (String): User name logged when the assignee/approver account is deleted
* **x\_dept** (String): Department name logged when the assignee/approver account is deleted

### Update Ticket Assignee Status

Updates the status of an assigned or submitted ticket.

#### HTTP Request

PUT /api/sonar/tickets/:guid/assignee-status

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d type=ASSIGNEE \ -d status=IN\_PROGRESS \ -X PUT \ https://HOSTNAME/api/sonar/tickets/6206eb0e-fb44-4f13-82ca-d92454cfd35e/assignee-status

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Ticket GUID | 36 characters |
| type | O | String | Role type | ASSIGNEE or APPROVER |
| status | O | String | Task status | For an assignee: ASSIGNED or IN\_PROGRESS or CLOSED. For an approver: APPROVED or REJECTED |

#### Success Response

{}

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Invalid assignee status

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "assignee status should be one of ASSIGNED, IN\_PROGRESS, CLOSED."}

Invalid approver status

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "approver status should be one of APPROVED, REJECTED."}

Ticket is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

Ticket is not assigned

{ "error\_code": "illegal-state", "error\_msg": "not assigned"}

Approve or reject an unsubmitted ticket

{ "error\_code": "illegal-state", "error\_msg": "cannot approve or reject unsubmitted ticket: 511ce7fe-36bd-45d8-a868-99a5349c3575"}

### Close Ticket

Updates the status of a specified ticket to Closed.

#### HTTP Request

POST /api/sonar/tickets/:guid/close

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/tickets/6206eb0e-fb44-4f13-82ca-d92454cfd35e/close

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Ticket GUID | 36 characters |

#### Success Response

{}

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Ticket is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

### Reopen Ticket

Reopens a specified ticket or updates the status to Assigned.

#### HTTP Request

POST /api/sonar/tickets/:guid/reopen

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/tickets/6206eb0e-fb44-4f13-82ca-d92454cfd35e/reopen

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Ticket GUID | 36 characters |

#### Success Response

{}

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Ticket is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

### Submit Ticket

Submits a ticket for approval.

#### HTTP Request

POST /api/sonar/tickets/:guid/submit

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/tickets/6206eb0e-fb44-4f13-82ca-d92454cfd35e/submit

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Ticket GUID | 36 characters |

#### Success Response

{}

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Ticket is not found

HTTP status code 500. Ticket repository privileges are required.

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

Approver is not assigned

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-approvers"}

No assignee privileges

HTTP status code 500. Only the assignee is allowed to submit the ticket.

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

Task is not completed yet

HTTP status code 500. Approval can only be requested for a ticket once the assigned task has been completed.

{ "error\_code": "illegal-state", "error\_msg": "not-completed"}

### Approve Ticket

Approves a submitted ticket.

#### HTTP Request

POST /api/sonar/tickets/:guid/approve

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/tickets/6206eb0e-fb44-4f13-82ca-d92454cfd35e/approve

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Ticket GUID | 36 characters |

#### Success Response

{}

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

No approver privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

Ticket is not submitted yet

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "cannot approve or reject unsubmitted ticket: c63ff706-85bc-44e3-9acd-24a0628da1fb"}

### Reject Ticket

Rejects a submitted ticket.

#### HTTP Request

POST /api/sonar/tickets/:guid/reject

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST \ https://HOSTNAME/api/sonar/tickets/6206eb0e-fb44-4f13-82ca-d92454cfd35e/reject

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Ticket GUID | 36 characters |

#### Success Response

{}

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

No approver privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

Ticket is not yet submitted

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "cannot approve or reject unsubmitted ticket: c63ff706-85bc-44e3-9acd-24a0628da1fb"}

### Get Ticket Attachments

#### HTTP Request

GET /api/sonar/tickets/:guid/attachments

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/tickets/8de3c683-a793-4bde-bf41-657396d17ef5/attachments

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Ticket GUID | 36 characters |

#### Success Response

{ "attachments": [ { "guid": "75624e2d-dc78-4a21-974b-78c2281dc089", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "ticket\_guid": "8de3c683-a793-4bde-bf41-657396d17ef5", "file\_name": "66c7e112-edc9-4b11-b332-5a0581a24211.png", "file\_size": 124109 } ]}

* **attachments** (Array): Attachment list
* **guid** (String): Attachment GUID
* **user\_guid** (String): User GUID
* **ticket\_guid** (String): Ticket GUID
* **file\_name** (String): File name
* **file\_size** (64-bit integer): File size

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Ticket is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 49272877-75f2-4c2f-9301-d21c4f9a106c"}

### Remove Ticket Attachment

Deletes the specified ticket attachment.

#### HTTP Request

DELETE /api/sonar/tickets/:ticket\_guid/attachments/:file\_guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ https://HOSTNAME/api/sonar/tickets/8de3c683-a793-4bde-bf41-657396d17ef5/attachments/75624e2d-dc78-4a21-974b-78c2281dc089

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| ticket\_guid | O | String | Ticket GUID | 36 characters |
| file\_guid | O | String | Attachment GUID | 36 characters |

#### Success Response

{}

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "ticket\_guid should be guid type."}

Ticket is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 49272877-75f2-4c2f-9301-d21c4f9a106c"}

Attachment is not found

{ "error\_code": "illegal-state", "error\_msg": "ticket attachment not found: 75624e2d-dc78-4a21-974b-78c2281dc089"}

### Get Ticket Comments

Get a list of the comments for a specified ticket.

#### HTTP Request

GET /api/sonar/tickets/:guid/comments

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/tickets/49272877-75f2-4c2f-9301-d21c4f9a106c/comments

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Ticket GUID | 36 characters |
| output\_html | X | Boolean | Whether to ouput as HTML | If not specified, output in original format. |

#### Success Response

{ "comments": [ { "guid": "b66a31b5-db94-478b-8751-194b5ee5f358", "user\_guid": "ffaf431b-653a-4329-8f83-913cbb00342d", "user\_name": "Joshua", "type": "TEXT", "format": "MARKDOWN", "content": "\* Blocked the IP address in firewall.", "created": "2022-09-14 17:52:20+0900", "updated": "2022-09-14 17:52:20+0900", "x\_login": null, "x\_user": null, "x\_dept": null } ]}

* (Array) comments
* **guid** (String): Guid of the ticket comment
* **user\_guid** (String): Author GUID
* **user\_name** (String): Author name
* **type** (String): (Reserved) Always TEXT.
* **format** (String): PLAIN or MARKDOWN.
* **content** (String): Comment content. If a user set the output\_html to true, MARKDOWN text will be output in HTML format.
* **created** (String): Date and time of creation (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Date and time of last modification (yyyy-MM-dd HH:mm:ssZ)
* **x\_login** (String): Login user name logged when the author's account is deleted
* **x\_user** (String): User name logged when the author's account is deleted
* **x\_dept** (String): Department name logged when the author's account is deleted

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Ticket is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 49272877-75f2-4c2f-9301-d21c4f9a106c"}

### Add Ticket Comment

Adds a comment to a specified ticket.

#### HTTP Request

POST /api/sonar/tickets/:ticket\_guid/comments

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d format=MARKDOWN \ -d content="\* Blocked the IP on the firewall" \ -X POST \ https://HOSTNAME/api/sonar/tickets/fa69e0dc-5116-491d-8a57-19cf0332b157/comments

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| ticket\_guid | O | String | Ticket GUID | 36 characters |
| guid | X | String | Note GUID | 36 characters |
| format | O | String | Content format | JSON or MARKDOWN or PLAIN |
| content | O | String | Content |  |

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Invalid format is specified

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "format should be one of PLAIN, MARKDOWN, JSON."}

Ticket is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

### Update Ticket Comment

Updates the comment of a specified ticket.

#### HTTP Request

PUT /api/sonar/tickets/:ticket\_guid/comments/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d format=MARKDOWN \ -d content="\* Blocked IP address" \ -X PUT \ https://HOSTNAME/api/sonar/tickets/fa69e0dc-5116-491d-8a57-19cf0332b157/comments/08ee89f1-630f-4b24-b6b2-e0c88c5f3003

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| ticket\_guid | O | String | Ticket GUID | 36 characters |
| guid | O | String | Note GUID | 36 characters |
| format | O | String | Content format | JSON or MARKDOWN or PLAIN |
| content | O | String | Content |  |

#### Success Response

{}

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Invalid format is specified

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "format should be one of PLAIN, MARKDOWN, JSON."}

Ticket is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "Ticket is not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

Ticket comment is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "ticket comment not found: 08ee89f1-630f-4b24-b6b2-e0c88c5f3002"}

### Remove Ticket Comment

Deletes the comment of a specified ticket.

#### HTTP Request

DELETE /api/sonar/tickets/:ticket\_guid/comments/:guid

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X DELETE \ https://HOSTNAME/api/sonar/tickets/fa69e0dc-5116-491d-8a57-19cf0332b157/comments/08ee89f1-630f-4b24-b6b2-e0c88c5f3003

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| ticket\_guid | O | String | Ticket GUID | 36 characters |
| guid | O | String | Note GUID | 36 characters |

#### Success Response

{}

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Ticket is not found

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "ticket not found: 201dc306-5ef7-4d4f-b872-1fa0f4d7dc57"}

### Get Explanation Templates

Gets a list of push template settings of the company (tenant) in the current session.

#### HTTP Request

GET /api/sonar/push-templates

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/push-templates

#### Success Response

{ "templates": { "sms\_explain\_req\_msg": "An explanation request for the $category case has been mailed to you. Due: $expire\_date", "sms\_explain\_review\_req\_msg": "The explanation review request for $emp\_name $emp\_title has been mailed to you. Due: $expire\_date" }}

* **templates** (Map): Template option key/value pairs

|  |  |
| --- | --- |
| Option Key | Description |
| explanation\_domain | Submission domain. https://DOMAIN format |
| mail\_explain\_req\_subject | Title of explanation request email |
| mail\_explain\_req\_body | Body of explanation request email |
| mail\_explain\_review\_req\_subject | Title of review request email |
| mail\_explain\_review\_req\_body | Boby of review request email |
| sms\_explain\_req\_msg | Explanation request SMS message |
| sms\_explain\_review\_req\_msg | Review request SMS message |

* You can use the following macros for template content:

|  |  |
| --- | --- |
| Macro | Description |
| $category | Category |
| $emp\_key | Employee number |
| $emp\_name | Employee name |
| $emp\_title | Employee title |
| $url | Submission URL |
| $expire\_date | Submission due date (yyyy-MM-dd) |
| $expire\_time | Submission due time (HH:mm:ss) |
| $user\_note | User note in case of auto-request |

### Get Push Template

Gets a specified push template setting of the company (tenant) in the current session.

#### HTTP Request

GET /api/sonar/push-templates/:type

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/push-templates/sms\_explain\_req\_msg

Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| type | O | String | Template type | Refer to the below table. |

Refer to the below table for available template types:

|  |  |
| --- | --- |
| Template type | Description |
| explanation\_domain | Submission domain. https://DOMAIN format |
| mail\_explain\_req\_subject | Title of explanation request email |
| mail\_explain\_req\_body | Boby of explanation request email |
| mail\_explain\_review\_req\_subject | Title of review request email |
| mail\_explain\_review\_req\_body | Boby of review request email |
| sms\_explain\_req\_msg | Explanation request SMS message |
| sms\_explain\_review\_req\_msg | Review request SMS message |

#### Success Response

{ "template": "An explanation request for the $category case has been mailed to you. Due: $expire\_date"}

* **template** (String): Template content
* You can use the following macros for template content:

|  |  |
| --- | --- |
| Macro | Description |
| $category | Category |
| $emp\_key | Employee number |
| $emp\_name | Employee name |
| $emp\_title | Employee title |
| $url | Submission URL |
| $expire\_date | Submission due date (yyyy-MM-dd) |
| $expire\_time | Submission due time (HH:mm:ss) |
| $user\_note | User note in case of auto-request |

#### Error Responses

Template type is not supported

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "type should be one of explanation\_domain, mail\_explain\_req\_subject, mail\_explain\_req\_body, mail\_explain\_review\_req\_subject, mail\_explain\_review\_req\_body, sms\_explain\_req\_msg, sms\_explain\_review\_req\_msg."}

### Set Push Template

Sets a push template of the company in the current session.

#### HTTP Request

POST /api/sonar/push-templates/:type

Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d template="$emp\_name $emp\_title, check your inbox for explanation request email." \ -X POST \ https://HOSTNAME/api/sonar/push-templates/sms\_explain\_req\_msg

Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| type | O | String | Template type |  |
| template | X | String | Template content | Maximum 16MB. If not specified, null (initialize). |

Refer to the below table for available template types:

|  |  |
| --- | --- |
| Template type | Description |
| explanation\_domain | Submission domain. https://DOMAIN format |
| mail\_explain\_req\_subject | Title of explanation request email |
| mail\_explain\_req\_body | Boby of explanation request email |
| mail\_explain\_review\_req\_subject | Title of review request email |
| mail\_explain\_review\_req\_body | Boby of review request email |
| sms\_explain\_req\_msg | Explanation request SMS message |
| sms\_explain\_review\_req\_msg | Review request SMS message |

Template content can include the below macros:

|  |  |
| --- | --- |
| Macro | Description |
| $category | Category |
| $emp\_key | Employee number |
| $emp\_name | Employee name |
| $emp\_title | Employee title |
| $url | Submission URL |
| $expire\_date | Submission due date (yyyy-MM-dd) |
| $expire\_time | Submission due time (HH:mm:ss) |
| $user\_note | User note in case of auto-request |

#### Success Response

{}

#### Error Responses

Template format is not supported

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "type should be one of explanation\_domain, mail\_explain\_req\_subject, mail\_explain\_req\_body, mail\_explain\_review\_req\_subject, mail\_explain\_review\_req\_body, sms\_explain\_req\_msg, sms\_explain\_review\_req\_msg."}

No privileges to set a template

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

## Scheduled Query API

### Get Scheduled Queries

Gets a list of the scheduled queries that match the search keyword. Administrator privileges are required to call this API.

#### HTTP Request

GET /api/sonar/scheduled-queries

#### Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/scheduled-queries

#### Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| offset | X | 32-bit integer | Number of records to skip | Default: 0 |
| limit | X | 32-bit integer | Maximum number of records to load | Default: all |
| keywords | X | String | Keywords | Search available by name, description, and query string |

#### Success Response

Below is a partial list of scheduled queries.

{ "total\_count": 15, "scheduled\_queries": [ { "guid": "95e17283-1d08-44f0-bac7-b734813d2dcd", "name": "test", "description": "", "enabled": false, "node\_types": null, "query": "json \"{}\"", "output\_parameter": false, "trigger\_type": "cron", "cron\_schedule": "\* \* \* \* \*", "preceding\_guid": null, "preceding\_name": null, "preceding\_action": null, "running\_state": null, "result\_state": null, "elapsed\_time": null, "last\_run\_time": null, "last\_failure\_time": null, "last\_failure\_reason": null, "created": "2023-09-18 16:12:44+0900", "updated": "2023-09-18 16:12:44+0900" } ]}

* **total\_count** (32-bit integer): total number of the scheduled queries that match the search keyword.
* **scheduled\_queries** (Array): Paged list of scheduled queries that match the search keyword
* **guid** (String): GUID of the scheduled query
* **name** (String): Name
* **description** (String): Description
* **enabled** (Boolean): Whether the scheduled query is enabled or not
* **node\_types** (Array): Node on which to run the query (control: control node, data: data node)
* **query** (String): Query string
* **output\_parameter** (Boolean): Whether to pass the last result row as query parameter(s) to the subsequent query
* **trigger\_type** (String): Query trigger (cron: Run at predefined intervals or on a predetermined schedule, workflow: Run based on the preceding query result)
* **cron\_schedule** (String): Cron schedule expression. Required when trigger\_type is set to cron.
* **preceding\_guid** (String): GUID of preceding query. Required when trigger\_type is set to workflow.
* **preceding\_name** (String): Name of preceding query. Required when trigger\_type is set to workflow.
* **preceding\_action** (String): Preceding query status. Either succeeded, failed, or finished when trigger\_type is set to workflow.
* **elapsed\_time** (32-bit integer): Elapsed time (unit: milliseconds)
* **running\_state** (String): Query running status. Either running, stopping, finished, or canceled.
* **result\_state** (String): Query result. Either succeeded, failed, or canceled.
* **last\_run\_time** (String): Last run time (yyyy-MM-dd HH:mm:ssZ)
* **last\_failure\_time** (String): Last failure time (yyyy-MM-dd HH:mm:ssZ)
* **last\_failure\_reason** (String): Query failure reason
* **created** (String): Creation time (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Last modified time (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

offset or limit value is not an integer

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'offset' must be greater than or equal to 0."}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Get Scheduled Query

Retrieves information of a specified scheduled query. Administrator privileges are required to call this API.

#### HTTP Request

GET /api/sonar/scheduled-queries/:guid

#### Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/scheduled-queries/95e17283-1d08-44f0-bac7-b734813d2dcd

#### Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Scheduled query GUID |  |

#### Success Response

{ "scheduled\_query": { "guid": "95e17283-1d08-44f0-bac7-b734813d2dcd", "name": "test", "description": "", "enabled": false, "node\_types": ["control", "data"], "query": "json \"{}\"", "output\_parameter": false, "trigger\_type": "cron", "cron\_schedule": "\* \* \* \* \*", "preceding\_guid": null, "preceding\_name": null, "preceding\_action": null, "running\_state": null, "result\_state": null, "elapsed\_time": null, "last\_run\_time": null, "last\_failure\_time": null, "last\_failure\_reason": null, "created": "2023-09-18 16:12:44+0900", "updated": "2023-09-18 16:12:44+0900" }}

* **scheduled\_query** (Map): Scheduled query
* **guid** (String): GUID of the scheduled query
* **name** (String): Name
* **description** (String): Description
* **enabled** (Boolean): Whether the scheduled query is enabled or not
* **node\_types** (Array): Node on which to run the query (control: control node, data: data node)
* **query** (String): Query string
* **output\_parameter** (Boolean): Whether to pass the last result row as query parameter(s) to the subsequent query
* **trigger\_type** (String): Query trigger (cron: Run at predefined intervals or on a predetermined schedule, workflow: Run based on the preceding query result)
* **cron\_schedule** (String): Cron schedule expression. Required when trigger\_type is set to cron.
* **preceding\_guid** (String): GUID of preceding query. Required when trigger\_type is set to workflow.
* **preceding\_name** (String): Name of preceding query. Required when trigger\_type is set to workflow.
* **preceding\_action** (String): Preceding query status. Either succeeded, failed, or finished when trigger\_type is set to workflow.
* **elapsed\_time** (32-bit integer): Elapsed time (unit: milliseconds)
* **running\_state** (String): Query running status. Either running, stopping, finished, or canceled.
* **result\_state** (String): Query result. Either succeeded, failed, or canceled.
* **last\_run\_time** (String): Last run time (yyyy-MM-dd HH:mm:ssZ)
* **last\_failure\_time** (String): Last failure time (yyyy-MM-dd HH:mm:ssZ)
* **last\_failure\_reason** (String): Query failure reason
* **created** (String): Creation time (yyyy-MM-dd HH:mm:ssZ)
* **updated** (String): Last modified time (yyyy-MM-dd HH:mm:ssZ)

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

Scheduled query is not found

HTTP status code 200

{ "result": false, "error\_msg": "scheduled query not found : 0fb16aa8-dbc1-458a-9769-342de5cf9211"}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Create Scheduled Query

Creates a new scheduled query. Administrator privileges are required to call this API.

#### HTTP Request

POST /api/sonar/scheduled-queries

#### Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="test" \ -d query="table duration=1m sonar\_cpu\_logs | search idle <= 10" \ -d type="cron" \ -d cron\_schedule="\* \* \* \* \*" \ -X POST https://HOSTNAME/api/sonar/scheduled-queries

#### Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| name | O | String | Name | Maximum 255 characters |
| description | X | String | Description | Maximum 2,000 characters |
| enabled | X | Boolean | Whether the scheduled query is enabled or not | Default: false |
| query | O | String | Query string |  |
| trigger\_type | O | String | Query trigger type | Either cron(Run at predefined intervals or on a predetermined schedule) or workflow(Run based on the preceding query result) |
| cron\_schedule | O | String | Cron expression | Required when trigger\_type is set to cron. |
| preceding\_guid | X | String | GUID of preceding query | Required when trigger\_type is set to workflow. |
| preceding\_action | X | String | Preceding query status | Either succeeded, failed, or finished when trigger\_type is set to workflow |
| node\_types | X | List of strings | Node on which to run the query | Comma-separated list of control(control node) or data(data node) |
| output\_parameter | X | Boolean | Whether to pass the last result row as query parameter(s) to the subsequent query | Default: false |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be shorter than or equal to 255 characters."}

Duplicated query name

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "duplicated name: test"}

Missing cron\_schedule value when trigger\_type is set to cron

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "cron\_schedule should be not null"}

Missing preceding\_action value when trigger\_type is set to workflow

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "preceding\_action should be not null"}

Invalid preceding\_action value when trigger\_type is set to workflow

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "preceding\_action value must be one of 'finished', 'succeeded', 'failed'."}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Update Scheduled Query

Updates a specified scheduled query. Administrator privileges are required to call this API.

#### HTTP Request

PUT /api/sonar/scheduled-queries/:guid

#### Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d name="test" \ -d query="table duration=1m sonar\_cpu\_logs | search idle <= 10" \ -d type="cron" \ -d cron\_schedule="\* \* \* \* \*" \ -X PUT https://HOSTNAME/api/sonar/scheduled-queries/95e17283-1d08-44f0-bac7-b734813d2dcd

#### Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Scheduled query GUID |  |
| name | O | String | Name | Maximum 255 characters |
| description | X | String | Description | Maximum 2,000 characters |
| enabled | X | Boolean | Whether the scheduled query is enabled or not | Default: false |
| query | O | String | Query string |  |
| trigger\_type | O | String | Query trigger type | Either cron(Run at predefined intervals or on a predetermined schedule) or workflow(Run based on the preceding query result) |
| cron\_schedule | O | String | Cron schedule expression | Required when trigger\_type is set to cron. |
| preceding\_guid | X | String | GUID of preceding query | Required when trigger\_type is set to workflow. |
| preceding\_action | X | String | Preceding query status | Either succeeded, failed, or finished when trigger\_type is set to workflow |
| node\_types | X | List of strings | Node on which to run the query | Comma-separated list of control(control node) or data(data node) |
| output\_parameter | X | Boolean | Whether to pass the last result row as query parameter(s) to the subsequent query | Default: false |

#### Success Response

{}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "name should be not null"}

Invalid argument length

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "'name' must be shorter than or equal to 255 characters."}

Duplicated query name

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "duplicated name: test"}

Missing cron\_schedule value when trigger\_type is set to cron

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "cron\_schedule should be not null"}

Missing preceding\_action value when trigger\_type is set to workflow

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "preceding\_action should be not null"}

Invalid preceding\_action value when trigger\_type is set to workflow

HTTP status code 400

{ "error\_code": "invalid-argument", "error\_msg": "preceding\_action value must be one of 'finished', 'succeeded', 'failed'."}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Remove Scheduled Queries

Deletes specified scheduled queries. Administrator privileges are required to call this API. This REST API supports partial failure. If any scheduled queries fail to be deleted, the failures parameter returns the identifiers of those scheduled queries and the failure reason.

#### HTTP Request

DELETE /api/sonar/scheduled-queries

#### Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids="GUID1,GUID2,GUIDN" -d policy="skip" -X DELETE https://HOSTNAME/api/sonar/scheduled-queries

#### Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guids | O | String | GUID list of scheduled queries | Comma-separated list |
| policy | X | String | Delete option | Either skip or force. (Default: skip) |

* skip: does not delete the scheduled query if it is running.
* force: stop and delete the scheduled query, even if it is running.

#### Success Responses

Successful Request

{ "succeeded": 1, "failures": []}

* (32-bit integer) succeeded: Total number of scheduled queries that have been successfully deleted. Any scheduled queries whose policy is skip are not included.
* (Array) failures: Failure details
* (String) id: GUID of the scheduled query
* (String) reason: Error description

Partial Successful Request

Request Example

curl -k -H "Authorization: Bearer API\_KEY" \ -d guids="0ff16aa8-dbc1-458a-9769-342de5cf9219,65c6c0d3-b8a4-49b3-b4ea-ddd0e321c221,b7007eb2-c1df-4d4d-84f1-5d0af91db25d" \ -X DELETE https://HOSTNAME/api/sonar/scheduled-query

Response Example

{ "succeed": 1, "failures": [ { "id": "0ff16aa8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "guids should be not null"}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

Scheduled query is not found

HTTP status code 200

{ "succeed": 0, "failures": [ { "id": "0fb16ff8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Enable Scheduled Query

Enables a specified scheduled query. Administrator privileges are required to call this API.

#### HTTP Request

POST /api/sonar/scheduled-queries/:guid/enable

#### Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST https://HOSTNAME/api/sonar/scheduled-queries/:guid/enable

#### Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Scheduled query GUID | 36 characters |

#### Success Response

{}

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guid should be guid type."}

GUID is not found

HTTP status code 200

{ "result": false, "error\_msg": "scheduled query not found : 0fb16aff-dbc1-458a-9769-342de5cf9219"}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Disable Scheduled Query

Disables a specified scheduled query. Administrator privileges are required to call this API.

#### HTTP Request

POST /api/sonar/scheduled-queries/:guid/disable

#### Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -X POST https://HOSTNAME/api/sonar/scheduled-queries/:guid/disable

#### Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guid | O | String | Scheduled query GUID | 36 characters |

#### Success Response

{}

#### Error Responses

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "guid should be not null"}

GUID is not found

HTTP status code 200

{ "result": false, "error\_msg": "scheduled query not found: 0fb16aff-dbc1-458a-9769-342de5cf9219"}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Enable Scheduled Queries

Enables specified scheduled queries. Administrator privileges are required to call this API. This REST API supports partial failure. If any scheduled queries fail to be disabled, the failures parameter returns the identifiers of those scheduled queries and the failure reason.

#### HTTP Request

POST /api/sonar/scheduled-queries/enable

#### Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids="GUID1,GUID2,GUIDN" \ -X POST https://HOSTNAME/api/sonar/scheduled-queries/enable

#### Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guids | O | String | GUID list of scheduled queries | Comma-separated list |

#### Success Response

Successful Request

{ "succeeded": 1, "failures": []}

* **succeeded** (32-bit integer): the total number of scheduled queries that have been successfully enabled, not including those already enabled.
* **failures** (Array): Failure details
* **id** (String): GUID of the scheduled query
* **reason** (String): Error description

Partial Successful Request

Request Example

curl -k -H "Authorization: Bearer API\_KEY" \ -d guids="0ff16aa8-dbc1-458a-9769-342de5cf9219,65c6c0d3-b8a4-49b3-b4ea-ddd0e321c221,b7007eb2-c1df-4d4d-84f1-5d0af91db25d" \ -X POST https://HOSTNAME/api/sonar/scheduled-queries/enable

Response Example

{ "succeeded": 2, "failures": [ { "id": "0ff16aa8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "guids should be not null"}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

Scheduled query is not found

HTTP status code 200

{ "succeeded": 0, "failures": [ { "id": "0fb16ff8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Disable Scheduled Queries

Disables specified scheduled queries. Administrator privileges are required to call this API. This REST API supports partial failure. If any scheduled queries fail to be disabled, the failures parameter returns the identifiers of those scheduled queries and the failure reason.

#### HTTP Request

POST /api/sonar/scheduled-queries/disable

#### Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids="GUID1,GUID2,GUIDN" -X POST https://HOSTNAME/api/sonar/scheduled-queries/disable

#### Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guids | O | String | GUID list of scheduled queries | Comma-separated list |

#### Success Responses

Successful Response

{ "succeeded": 1, "failures": []}

* **succeeded** (32-bit integer): the total number of scheduled queries that have been successfully disabled, not including those already disabled.
* **failures** (Array): Failure details
* **id** (String): GUID of the scheduled query
* **reason** (String): Error description

Partial Successful Response

Request Example

curl -k -H "Authorization: Bearer API\_KEY" \ -d guids="0ff16aa8-dbc1-458a-9769-342de5cf9219,65c6c0d3-b8a4-49b3-b4ea-ddd0e321c221,b7007eb2-c1df-4d4d-84f1-5d0af91db25d" \ -X POST https://HOSTNAME/api/sonar/scheduled-queries/disable

Response Example

{ "succeeded": 2, "failures": [ { "id": "0ff16aa8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "guids should be not null"}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

Scheduled query is not found

HTTP status code 200

{ "succeeded": 0, "failures": [ { "id": "0fb16ff8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Run Scheduled Queries

Runs specified scheduled queries. Administrator privileges are required to call this API. This REST API supports partial failure. If any scheduled queries fail to be disabled, the failures parameter returns the identifiers of those scheduled queries and failure reason.

#### HTTP Request

POST /api/sonar/scheduled-queries/run

#### Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids="GUID1,GUID2,GUIDN" \ -X POST https://HOSTNAME/api/sonar/scheduled-queries/run

#### Request Parameters

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guids | O | String | GUID list of scheduled queries | Comma-separated list |
| policy | X | String | Handling option when there is an already running query | Either skip or restart. Default: skip |

* skip: skip already running queries.
* restart: stop and restart already running queries.

#### Success Response

Successful Request

{ "succeeded": 1, "failures": []}

* **succeeded** (32-bit integer): the total number of scheduled queries that have been successfully executed, not including scheduled queries that were already in the running state.
* **failures** (Array): Failure details
* **id** (String): GUID of the scheduled query
* **reason** (String): Error description

Partial Successful Request

Request Example

curl -k -H "Authorization: Bearer API\_KEY" \ -d guids="0ff16aa8-dbc1-458a-9769-342de5cf9219,65c6c0d3-b8a4-49b3-b4ea-ddd0e321c221,b7007eb2-c1df-4d4d-84f1-5d0af91db25d" \ -X POST https://HOSTNAME/api/sonar/scheduled-queries/run

Response Example

{ "succeeded": 2, "failures": [ { "id": "0ff16aa8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "guids should be not null"}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

Scheduled query is not found

HTTP status code 200

{ "succeeded": 0, "failures": [ { "id": "0fb16ff8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}

### Stop Scheduled Queries

Stops specified scheduled queries. Administrator privileges are required to call this API. This REST API supports partial failure. If any scheduled queries fail to be disabled, the failures parameter returns the identifiers of those scheduled queries and the failure reason.

#### HTTP Request

POST /api/sonar/scheduled-queries/stop

#### Request using cURL

curl -H "Authorization: Bearer <API\_KEY>" \ -d guids="GUID1,GUID2,GUIDN" -X POST https://HOSTNAME/api/sonar/scheduled-queries/stop

#### Request Parameter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Key | Required | Type | Description | Note |
| guids | O | String | GUID list of scheduled queries | Comma-separated list |

#### Success Response

Successful Request

{ "succeeded": 1, "failures": []}

* **succeeded** (32-bit integer): the total number of scheduled queries that have been successfully stopped, not including those already stopped.
* **failures** (Array): Failure details
* **id** (String): GUID of the scheduled query
* **reason** (String): Error description

Partial Successful Request

Request Example

curl -k -H "Authorization: Bearer API\_KEY" \ -d guids="0ff16aa8-dbc1-458a-9769-342de5cf9219,65c6c0d3-b8a4-49b3-b4ea-ddd0e321c221,b7007eb2-c1df-4d4d-84f1-5d0af91db25d" \ -X POST https://HOSTNAME/api/sonar/scheduled-queries/stop

Response Example

{ "succeeded": 2, "failures": [ { "id": "0ff16aa8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

#### Error Responses

Required argument is missing

HTTP status code 400

{ "error\_code": "null-argument", "error\_msg": "guids should be not null"}

Identifier is not in valid GUID format

HTTP status code 400

{ "error\_code": "invalid-param-type", "error\_msg": "guids should be guid type."}

Scheduled query is not found

HTTP status code 200

{ "succeeded": 0, "failures": [ { "id": "0fb16ff8-dbc1-458a-9769-342de5cf9219", "reason": "scheduled-query-not-found" } ]}

No administrator privileges

HTTP status code 500

{ "error\_code": "illegal-state", "error\_msg": "no-permission"}