### 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"}