### 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}