

Extract metrics through the REST API

Published: 2024-04-02


You can extract metrics from a sensor or console through the REST API to visualize metrics in a third-party tool or compare ExtraHop data with other data you have collected. To extract a metric, you must first get identifiers for both the metrics you want to extract and the objects you want to extract metrics for. You can then build and test a metric query in the REST API Explorer before incorporating your request into a script that can read the metrics into a format that can be imported into applications.

Before you begin

- For sensors and ECA VMs, you must have a valid API key to make changes through the REST API and complete the procedures below. (See [Generate an API key](#).)
- For Reveal(x) 360, you must have valid REST API credentials to make changes through the REST API and complete the procedures below. (See [Create REST API credentials](#).)

Retrieve metric IDs

Metrics are identified in the ExtraHop REST API through a combination of the `metric_category`, the `name`, and the `object_type`. You can retrieve all three identifiers through the Metric Explorer.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon  and then click **Metric Catalog**.
3. In the Type to filter field, type the name of the metric you want to extract and then click the name of the metric in the search results below.
4. In the right pane, scroll down to REST API parameters and record the values.

For example, the following information is displayed for the HTTP server responses metric:

REST API Parameters

```
{
  "metric_category": "http_server",
  "object_type": "device",
  "metric_specs": [
    {
      "name": "rsp"
    }
  ]
}
```

Retrieve object IDs

Next, you must find the unique identifier for the object that you want to extract metrics for in the REST API. You can retrieve this ID through the REST API Explorer.

 **Important:** The REST API Explorer is not available on Reveal(x) 360.

1. In a browser, navigate to the REST API Explorer.

The URL is the hostname or IP address of your sensor or console, followed by `/api/v1/explore/`. For example, if your hostname is `seattle-eda`, the URL is `https://seattle-eda/api/v1/explore/`.

2. Click **Enter API Key** and then paste or type your API key into the **API Key** field.
3. Click **Authorize** and then click **Close**.
4. Click the type of object you want to collect metrics for, such as **Device**, **Device Group**, **Application**, or **Appliance**.
5. Click **GET /<objects>**.
For example, if you are extracting metrics for a device group, click **Get/ Device Groups**.
6. Click **Try it out**.
7. Optional: In the Parameters section, specify search criteria for the object you want to locate.
For example, you can search for object names, IP addresses, or MAC addresses. If you are having difficulty locating a device, see [Find a device](#).
8. Click **Send Request**.
In the Server response section, the Response Body displays information about each object that matches the search criteria.
9. Note the number in the id field for the object you want to collect metrics for.
For example, the id of the following server is 1298:

```
[
  {
    "mod_time": 1516639693474,
    "node_id": null,
    "id": 1298,
    "extrahop_id": "fff4c3090a0a0000",
    "discovery_id": "fff4c3090a0a0000",
    "display_name": "server1",
    "description": null,
    "user_mod_time": 1512688149084,
    "discover_time": 1498685400000,
    "vlanid": 0,
    "parent_id": 140,
    "macaddr": "A1:01:01:01:1A:01",
    "vendor": "Mellanox",
    "is_l3": true,
    "ipaddr4": "10.10.10.200",
    "ipaddr6": null,
    "device_class": "node",
    "default_name": "Mellanox 10.10.10.200",
    "custom_name": "server1",
    "cdp_name": "",
    "dhcp_name": "server1.company.com",
    "netbios_name": "",
    "dns_name": "server1.company.com",
    "custom_type": "",
    "analysis_level": 1,
    "activity": []
  }
]
```

Query for metrics

You can query metrics through the REST API Explorer to make sure you have configured the right request body before adding the request to a script.

 **Important:** The REST API Explorer is not available on Reveal(x) 360.

1. In the REST API Explorer, click **Assets**, and then click **POST /metrics**.
2. Click **Try it out**.

3. In the body field, specify the metric that you want to extract.

For example, the following body extracts five minute metrics on HTTP responses for a server with an ID of 1298:

```
{
  "metric_category": "http_server",
  "metric_specs": [
    {
      "name": "rsp"
    }
  ],
  "object_type": "device",
  "object_ids": [
    1298
  ],
  "cycle": "5min"
}
```

The body must include the following parameters:


- **object_type:** The type of object you want to collect metrics for.
 - **object_ids:** The id of the object you want to extract metrics for.
 - **metric_category:** The category of the metric you want to collect.
 - **name:** The name of the metric you want to collect.
 - **cycle:** The aggregation period for metrics.
4. Click **Send Request** to send the request to your sensor or console.
In the Server response section, the Response body displays the requested metrics in JSON format.

Retrieve and run the example Python script

The ExtraHop GitHub repository contains an example Python script that extracts the total count of HTTP responses a server with an ID of 1298 sent over five minute time intervals and then writes the values to a CSV file.

1. Go to the [ExtraHop code-examples GitHub repository](#) and download the `extract_metrics/extract_metrics.py` file to your local machine.
2. In a text editor, open the `extract_metrics.py` file and replace the configuration variables with information from your environment.
 - For sensors and ECA VMs, specify the following configuration variables:
 - **HOST:** The IP address or hostname of the sensor or ECA VM.
 - **API_KEY:** The API key.
 - For Reveal(x) 360, specify the following configuration variables:
 - **HOST:** The hostname of the Reveal(x) 360 API. This hostname is displayed in the Reveal(x) 360 API Access page under API Endpoint. The hostname does not include the `/oauth2/token`.
 - **ID:** The ID of the Reveal(x) 360 REST API credentials.
 - **SECRET:** The secret of the Reveal(x) 360 REST API credentials.
3. Run the following command:

```
python3 extract_metrics.py
```

 **Note:** If the script returns an error message that the SSL certificate verification failed, make sure that [a trusted certificate has been added to your sensor or console](#). Alternatively,

you can add the `verify=False` option to bypass certificate verification. However, this method is not secure and not recommended. The following code sends an HTTP GET request without certificate verification:

```
requests.get(url, headers=headers, verify=False)
```