Search for a device through the REST API

Published: 2023-04-22

You can search through all discovered devices on your sensor or console by specifying your criteria (such as IP address or discovery ID) and then export the list of devices and their associated metadata to a file format that is readable through a third-party application like Microsoft Excel or any CSV reader. For example, you might want to view and export the IP addresses of each VMware device on your network.

You can test device search queries before incorporating them into a script by running the queries in the ExtraHop REST API Explorer. This guide includes methods for both the REST API Explorer and a sample Python script.

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.)

Search for a device 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 **Device** to display device operations.
5. Click **POST /devices/search**.
6. Click **Try it out**.
   The JSON schema is automatically added to the body parameter text box.
7. In the body text box, type your search criteria.
   The following search criteria returns a device with an IP address of 10.10.10.200:

```
{
  "filter": {
    "field": "ipaddr",
    "operand": "10.10.10.200",
    "operator": "="
  }
}
```

Retrieve and run the example Python script

The ExtraHop GitHub repository contains an example Python script that searches for a list of devices by IP address. The script then outputs the ExtraHop discovery ID for each IP address.

1. Go to the ExtraHop code-examples GitHub repository and download the `search_device/search_device.py` file to your local machine.
2. In a text editor, open the `search_device.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.
  - **IP_ADDR_LIST:** An array of IP addresses.
- 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 `/oauth/token`.
  - **ID:** The ID of the Reveal(x) 360 REST API credentials.
  - **SECRET:** The secret of the Reveal(x) 360 REST API credentials.
  - **IP_ADDR_LIST:** An array of IP addresses.

3. Run the following command:

```
python3 search_device.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)
```