ExtraHop 9.5
Reveal(x) 360 REST API Guide

For more documentation, see https://docs.extrahop.com.

Published: 2024-02-28

ExtraHop Networks
Seattle, WA 98101
877-333-9872 (US)
+44 (0)203 7016850 (EMEA)
+65-31585513 (APAC)
www.extrahop.com

Contents

Reveal(x) 360 REST API Guide

The Reveal(x) 360 REST API enables you to automate configuration tasks and retrieve metrics, packets, and detections from Reveal(x) 360. You can send requests to the API through a Representational State Transfer (REST) interface, which is accessed through resource URIs and standard HTTP methods.

Before you can send a REST API request to Reveal(x) 360, you must enable the system for REST API access and generate credentials. Then, you must retrieve a temporary access token by sending the ID and secret of your REST API credentials to Reveal(x) 360. Finally, include the access token in the header of your request for authentication. REST API credentials do not expire automatically and must be manually deleted before they become invalid.

Note: This guide is intended for an audience that has a basic familiarity with software development and the ExtraHop system.

Enable the REST API for Reveal(x) 360

Before you can send REST API requests to Reveal(x) 360, you must enable REST API access.

Before you begin

- You must have system and access administration privileges.

1. Log in to Reveal(x) 360.
2. Click the System Settings icon at the top right of the page and then click **All Administration**.
3. Click **API Access**.
4. In the Manage API Access section, click **Enable**.

   If you disable and then re-enable the REST API, the REST API might be unavailable for approximately 15 minutes due to DNS propagation, even if the Status section indicates that access is enabled. We recommend that you do not disable and re-enable the REST API often.

Create REST API credentials

Reveal(x) 360 authenticates REST API requests with the OpenID Connect (OIDC) protocol. OIDC requires users to provide temporary access tokens when making a request to the API. Before you can generate access tokens, you must create REST API credentials, also known as client credentials.

Note: REST API credentials do not expire automatically. The credentials created by a user are not deleted when the user is removed from the system. The credentials remain valid until deleted. Any administrator can delete any credentials, regardless of which user created the credentials.

The Reveal(x) 360 REST API does not support cross-origin resource sharing (CORS).

Before you begin

- You must have system and access administration privileges.

1. Log in to Reveal(x) 360.
2. Click the System Settings icon at the top right of the page and then click **All Administration**.
3. Click **API Access**.
4. Click **Create Credentials**.
5. In the **Name** field, type a name for the credentials.
6. In the **Privileges** field, specify a privilege level for the credentials.

   The privilege level determines which actions can be performed with the credential. Do not grant more privileges to REST API credentials than needed because it can create a security risk. For example, applications that only retrieve metrics should not be granted credentials that grant administrative privileges. For more information about each privilege level, see User privileges.

   Note: System and Access Administration privileges are similar to Full write privileges and allow the credentials to connect self-managed sensors and Trace appliances to Reveal(x) 360.
7. In the **Packet Access** field, specify whether you can retrieve packets and session keys with the credentials.
8. Click **Save**.
   The Copy REST API Credentials pane appears.
9. Under ID, click **Copy to Clipboard** and save the ID to your local machine.
10. Under Secret, click **Copy to Clipboard** and save the secret to your local machine.

    Important: The secret cannot be viewed or retrieved later.
11. Click **Done**.

Generate a REST API token

A temporary API access token must be included with all REST API requests to Reveal(x) 360. After you create REST API credentials, you can write scripts that generate temporary API access tokens with the credentials. The scripts can then authenticate REST API requests to Reveal(x) 360 with the tokens. Tokens are valid for 10 minutes after being generated.

The HTTPS token request must meet the following requirements:

- The token is sent in a POST request to the API token endpoint, which is displayed on the API Access page under API Endpoint in Reveal(x) 360.
- Include the following headers:
  - `Authorization: Basic <auth>`

    Where `<auth>` is a base64 encoded string of the ID and secret joined by a colon.
  - `Content-Type: application/x-www-form-urlencoded`
- Include the following payload:

```
grant_type=client_credentials
```

Note: The temporary API access tokens created by the example scripts are only valid for 10 minutes. If a script takes longer than 10 minutes to run, the script must generate a new token every 10 minutes to ensure that it does not send an expired token. If a script sends an expired token, the system responds with a 401 HTTP error code and the following error message:

```
The incoming token has expired
```

Next steps
After you generate a token, you can include it as a bearer token in the HTTP authorization header to authenticate requests. For example, if your token is "`abcdefghijklmnop0123456789`", include the following string in the header:

```
"Authorization": "Bearer abcdefghijklmnop0123456789"
```

Retrieve and run the example Python script

The ExtraHop GitHub repository contains an example Python script that generates a temporary API access token and then authenticates two simple requests with the token that retrieve devices and device groups from Reveal(x) 360.

1. Go to the ExtraHop code-examples GitHub repository and download the `py_rx360_auth/py_rx360_auth.py` file to your local machine.
2. In a text editor, open the `py_rx360_auth.py` file and replace the following configuration variables with information from your environment:

   • **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 REST API credentials.

   • **SECRET:** The secret of the REST API credentials.

   Run the following command:

```
python3 py_rx360_auth.py
```

Bash and cURL example

The ExtraHop GitHub repository contains an example Bash script that generates a REST API token with the cURL command and then authenticates two simple requests with the token that retrieve devices and device groups from the Reveal(x) 360 REST API.

Before you begin

- The cURL tool must be installed on your machine.
- The jq parser must be installed on your machine. For more information, see https://stedolan.github.io/jq/.

1. Go to the ExtraHop code-examples GitHub repository and download the `bash_rx360_auth/bash_rx360_auth.sh` file to your local machine.
2. In a text editor, open the `bash_rx360_auth.sh` file and replace the following configuration variables with information from your environment:

   • **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 REST API credentials.

   • **SECRET:** The secret of the REST API credentials.
3. Run the following command:

```
./bash_auth.sh
```

Learn about the REST API Explorer

The REST API Explorer is a web-based tool that enables you to view detailed information about the ExtraHop REST API resources, methods, parameters, properties, and error codes. Code samples are available in Python, cURL, and Ruby for each resource. You also can perform operations directly through the tool.

Open the REST API Explorer

You can open the REST API Explorer from the Administration settings or through the following URL:

```
https://<revealx-360-hostname-or-ip-address>/api/v1/explore/
```

1. Log in to Reveal(x) 360.
2. Click the System Settings icon at the top right of the page and then click **All Administration**.
3. Click **API Access**.
4. On the API Access page, click **Open ExtraHop REST API Explorer**.
   The REST API Explorer opens in your browser.

View operation information

From the REST API Explorer, you can click any operation to view configuration information for the resource.

The following table provides information about the sections available for resources in the REST API Explorer. Section availability varies by HTTP method. Not all methods have all of the sections listed in the table.

Section	Description
Body Parameters	Provides all of the fields for the request body and supported values for each field.
Parameters	Provides information about the available query parameters.
Responses	Provides information about the possible HTTP status codes for the resource. If you click **Send Request**, this section also includes the response from the server and the cURL, Python, and Ruby syntax required to send the specified request. **Tip:** Click **Model** to view descriptions of the fields returned in a response.

Identify objects on the ExtraHop system

Objects on the ExtraHop system can be identified by any unique value, such as the IP address, MAC address, name, or system ID. However, to perform API operations on a specific object, you must locate the object ID. You can easily locate the object ID through the following methods in the REST API Explorer.

- The object ID is provided in the headers returned from a POST request. For example, if you send a POST request to create a page, the response headers display a location URL.

The following request returned the location for the newly created tag as `/api/v1/tags/1` and the ID for the tag as `1`.

```
{
 "date": "Tue, 09 Nov 2021 18:21:00 GMT ",
 "via": "1.1 localhost",
 "server": "Apache",
 "content-type": "text/plain; charset=utf-8",
 "location": "/api/v1/tags/1",
 "cache-control": "private, max-age=0",
 "connection": "Keep-Alive",
 "keep-alive": "timeout=90, max=100",
 "content-length": "0"
}
```

- The object ID is provided for all objects returned from a GET request. For example, if you perform a GET request on all devices, the response body contains information for each device, including the ID.

  The following response body displays an entry for a single device, with an ID of 10212:

```
{
 "mod_time": 1448474346504,
 "node_id": null,
 "id": 10212,
 "extrahop_id": "test0001",
 "description": null,
 "user_mod_time": 1448474253809,
 "discover_time": 1448474250000,
 "vlanid": 0,
 "parent_id": 9352,
 "macaddr": "00:05:G3:FF:FC:28",
 "vendor": "Cisco",
 "is_l3": true,
 "ipaddr4": "10.10.10.5",
 "ipaddr6": null,
 "device_class": "node",
 "default_name": "Cisco5",
 "custom_name": null,
 "cdp_name": "",
 "dhcp_name": "",
 "netbios_name": "",
 "dns_name": "",
 "custom_type": "",
 "analysis_level": 1
},
```

- The object ID is provided in the URL for most objects. For example, in the ExtraHop system, click on **Assets**, and then **Devices**. Select any device and view the URL. In the following example, the URL for the device page shows Oid=10180.

```
https://10.10.10.205/extrahop/#/Devices?details=true&device
Oid=10180&from=6&interval_type=HR&until=0&view=l2stats
```

  To perform specific requests for that device, add 10180 to the id field in the REST API Explorer or to the body parameter in your request.

  The URL for dashboards displays a short_code, which appears after /Dashboard. When you add the short_code to the REST API Explorer or to your request, you must prepend a tilde to the short code.

In the following example, kmC9Y is the short_code. To perform requests for this dashboard, add ~kmC9Y as the value for the short_code field.

```
https://10.10.10.205/extrahop/#/Dashboard/kmC9Y/?from=6&interval_
type=HR&until=0
```

You can also find the short_code and dashboard ID in the Dashboard Properties for any dashboard, which can be accessed from the command menu ⋮. Some API operations, such as DELETE, require the dashboard ID.

Reveal(x) 360 resources

You can perform operations on the following resources through the Reveal(x) 360 REST API. You also can also view more detailed information about these resources, such as available HTTP methods, query parameters, and object properties.

Note: API endpoints are located at `<host>/api/v1/<endpoint>`, where `host` is the hostname of the Reveal(x) 360 API. For example, if the hostname of the API is `https://example.com`, the endpoint for activity maps would be the following URL:

`https://example.com/api/v1/activitymaps`

You can derive the hostname from the API token endpoint by removing `/oauth2/token` from the endpoint string, which appears on the Reveal(x) 360 API Access page under API Endpoint.

Activity Map

An activity map is a dynamic visual representation of the L4-L7 protocol activity between devices in your network. Create a 2D or 3D layout of device connections in real-time to learn about the traffic flow and relationships between devices.

Here are some important considerations about activity maps:

- You can only create activity maps for devices in Standard Analysis and Advanced Analysis. Discovery Mode devices are not included in activity maps. For more information, see Analysis levels.
- If you create an activity map for a device, activity group, or device group with no protocol activity in the selected time interval, the map appears without any data. Change the time interval or your origin selection and try again.
- You can create an activity map in a console to view device connections across all of your sensors.

To learn about configuring and navigating activity maps, see Activity maps.

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /activitymaps	Retrieve all activity maps.
POST /activitymaps	Create a new activity map.
POST /activitymaps/query	Perform a network topology query, which returns activity map data in flat file content.
DELETE /activitymaps/{id}	Delete a specific activity map.
GET /activitymaps/{id}	Retrieve a specific activity map.
PATCH /activitymaps/{id}	Update a specific activity map.
POST /activitymaps/{id}/query	Perform a topology query for a specific activity map, which returns activity map data in flat file content.
GET /activitymaps/{id}/sharing	Retrieve the users and their sharing permissions for a specific activity map.
PATCH /activitymaps/{id}/sharing	Update the users and their sharing permissions for a specific activity map.

Operation	Description
PUT /activitymaps/{id}/sharing	Replace the users and their sharing permissions for a specific activity map.

Operation details

`POST /activitymaps`

Specify the following parameters.

`body:` ***Object***

The activity map properties.

`name:` ***String***

The friendly name for the activity map.

`short_code:` ***String***

(Optional) The unique short code that is global to all activity maps.

`description:` ***String***

The description for the activity map.

`weighting:` ***String***

(Optional) The metric value that determines how activity is weighted between devices. Supported element values are "bytes", "connections", and "turns".

`mode:` ***String***

(Optional) The layout of the activity map. Supported values are "2dforce" and "3dforce".

`show_alert_status:` ***Boolean***

(Optional) Indicates whether to show the alert status for devices on the activity map. If enabled, the color of each device on the map represents the most severe alert level associated with the device.

`walks:` ***Array of Objects***

The list of one or more walk objects. A walk is the path of traffic composed of one or more steps. Each walk begins with one or more origin devices and expands to connections to peer devices that are based on protocol activity. Each expansion from the origin is a step. The contents of the object are defined in the "walk" section below.

`origins:` ***Array of Objects***

The list of one or more origin devices of the first step within the walk. Object contents are defined in the "source_object" section below.

`object_type:` ***String***

The metric source type.

The following values are valid:

- `device`
- `device_group`

`object_id:` ***Number***

The unique identifier for the source object.

`steps:` ***Array of Objects***

The list of one or more steps within the walk. Each step is defined by the protocol activity between devices of the previous step to a new set of peer devices. Object contents are defined in the "step" section below.

`relationships:` ***Array of Objects***

(Optional) The list of one or more filters that define the relationship between two devices. The filters specify which roles and protocols to search for when locating peer devices in the step. Relationships are represented as an edge in the activity map. Object contents are defined in the "relationship" section below. If no value is specified, the operation will locate all peers.

`protocol:` ***String***

(Optional) The metric protocol associated with the relationship, such as "HTTP" or "DNS". The operation only locates connections between devices over the specified protocol.

`role:` ***String***

(Optional) The device role associated with the metric protocol of the relationship. The operation only locates connections between devices over the associated protocol in the specified role. Supported role values are "client", "server", or "any". Set to "any" to locate all client, server, and peer device relationships associated with the specified protocol.

`peer_in:` ***Array of Objects***

(Optional) The list of one or more peer device objects to include in the activity map. Only relationships to peers of the specified source object are included. Object contents are defined in the "source_object" section below.

`object_type:` ***String***

The metric source type.

The following values are valid:

- `device`
- `device_group`

`object_id:` ***Number***

The unique identifier for the source object.

`peer_not_in:` ***Array of Objects***

(Optional) The list of one or more peer device objects to exclude from the activity map. Relationships to peers of the specified source object are excluded. Object contents are defined in the "source_object" section below.

`object_type:` ***String***

The metric source type.

The following values are valid:

- `device`
- `device_group`

`object_id:` ***Number***

The unique identifier for the source object.

Specify the body parameter in the following JSON format.

```
{
    "description": "string",
    "mode": "string",
    "name": "string",
    "short_code": "string",
    "show_alert_status": true,
    "walks": {
        "origins": {
            "object_type": "string",
            "object_id": 0
```

```
        },
        "steps": {
            "relationships": {
                "protocol": "string",
                "role": "string"
            },
            "peer_in": {
                "object_type": "string",
                "object_id": 0
            },
            "peer_not_in": {
                "object_type": "string",
                "object_id": 0
            }
        }
    },
    "weighting": "string"
}
```

`POST /activitymaps/query`

Specify the following parameters.

`body:` ***Object***

The topology query properties.

`from:` ***Number***

The beginning timestamp of the time range the query will search, expressed in milliseconds since the epoch.

`until:` ***Number***

(Optional) The ending timestamp of the time range the query will search, expressed in milliseconds since the epoch. If no value is set, the query end defaults to "now".

`weighting:` ***String***

(Optional) The metric value that determines how activity is weighted between devices.

The following values are valid:

- `bytes`
- `connections`
- `turns`

`edge_annotations:` ***Array of Strings***

(Optional) The list of one or more edge annotations to include in the topology query.

The following values are valid:

- `protocols`
- `appearances`

`walks:` ***Array of Objects***

The list of one or more walk objects to include in the topology query. A walk is the path of traffic composed of one or more steps. Each walk begins with one or more origin devices and expands to connections to peer devices that are based on protocol activity. Each expansion from the origin is a step. Object contents are defined in the "topology_walk" section below.

`origins:` ***Array of Objects***

The list of one or more origin devices of the first step within the walk. Object contents are defined in the "topology_source" section below.

`object_type:` ***String***

The type of source object.

The following values are valid:

- `all_devices`
- `device_group`
- `device`

`object_id:` ***Number***

The unique identifier for the source object. Set to 0 if the value of the "object_type" parameter is "all_devices".

`steps:` ***Array of Objects***

The list of one or more steps within the walk. Each step is defined by the protocol activity between devices of the previous step to a new set of peer devices. Object coontents are defined in the "topology_step" section below.

`relationships:` ***Array of Objects***

(Optional) The list of one or more filters that define the relationship between two devices. The filters specify which roles and protocols to search for when locating peer devices in the step. Relationships are represented as an edge in the activity map. If no value is set, the operation includes all peers. Object contents are defined in the "topology_relationship" section below.

`role:` ***String***

(Optional) The role of the peer device in relation to the origin device.

The following values are valid:

- `client`
- `server`
- `any`

`protocol:` ***String***

(Optional) The protocol over which the origin device is communicating, such as "HTTP". If no value is set, the object includes any protocol.

`peer_in:` ***Array of Objects***

(Optional) The list of one or more peer devices to include in the topology graph. Only relationships to peers of the specified source object are included. Object contents are defined in the "topology_source" section below.

`object_type:` ***String***

The type of source object.

The following values are valid:

- `all_devices`
- `device_group`
- `device`

`object_id:` ***Number***

The unique identifier for the source object. Set to 0 if the value of the "object_type" parameter is "all_devices".

`peer_not_in:` ***Array of Objects***

(Optional) The list of one or more peer devices to exclude from the topology graph. Relationships to peer devices of the specified source object are excluded. Object contents are defined in the "topology_source" section below.

`object_type:` ***String***

The type of source object.

The following values are valid:

- `all_devices`

- `device_group`
- `device`

`object_id`: ***Number***

The unique identifier for the source object. Set to 0 if the value of the "object_type" parameter is "all_devices".

Specify the body parameter in the following JSON format.

```
{
    "edge_annotations": [],
    "from": 0,
    "until": 0,
    "walks": {
        "origins": {
            "object_type": "string",
            "object_id": 0
        },
        "steps": {
            "relationships": {
                "role": "string",
                "protocol": "string"
            },
            "peer_in": {
                "object_type": "string",
                "object_id": 0
            },
            "peer_not_in": {
                "object_type": "string",
                "object_id": 0
            }
        }
    },
    "weighting": "string"
}
```

`GET /activitymaps`

There are no parameters for this operation.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "description": "string",
    "id": 0,
    "mod_time": 0,
    "mode": "string",
    "name": "string",
    "owner": "string",
    "rights": [
        "string"
    ],
    "short_code": "string",
    "show_alert_status": true,
    "walks": [],
    "weighting": "string"
}
```

`GET /activitymaps/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the activity map.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "description": "string",
    "id": 0,
    "mod_time": 0,
    "mode": "string",
    "name": "string",
    "owner": "string",
    "rights": [
        "string"
    ],
    "short_code": "string",
    "show_alert_status": true,
    "walks": [],
    "weighting": "string"
}
```

`POST /activitymaps/{id}/query`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the activity map.

`body:` ***Object***

The topology query properties.

`from:` ***Number***

The beginning timestamp of the time range the query will search, expressed in milliseconds since the epoch.

`until:` ***Number***

(Optional) The ending timestamp of the time range the query will search, expressed in milliseconds since the epoch. If no value is set, the query end defaults to "now".

`edge_annotations:` ***Array of Strings***

(Optional) The list of one or more edge annotations to include in the topology query.

The following values are valid:

- `protocols`
- `appearances`

Specify the body parameter in the following JSON format.

```
{
    "edge_annotations": [],
    "from": 0,
    "until": 0
}
```

`DELETE /activitymaps/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the activity map.

`PATCH /activitymaps/{id}`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the activity map.

`body:` ***Object***
The activity map properties to update.

`GET /activitymaps/{id}/sharing`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the activity map.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "anyone": "string",
    "groups": {},
    "users": {}
}
```

`PUT /activitymaps/{id}/sharing`

Specify the following parameters.

`body:` ***Object***
The users and their permission levels.

`id:` ***Number***
The unique identifier for the activity map.

`PATCH /activitymaps/{id}/sharing`

Specify the following parameters.

`body:` ***Object***
The users and their permission levels.

`id:` ***Number***
The unique identifier for the activity map.

Alert

Alerts are system notifications that are generated upon specified alert criteria. Default alerts are available in the system, or you can create a custom alert.

Detections and threshold alerts can be set to alert you if a metric crosses the value defined in the alert configuration. Trend alerts cannot be configured through the REST API. For more information, see Alerts.

Note: Machine learning detections require a connection to ExtraHop Cloud Services.

The following table displays all of the operations you can perform this resource:

Operation	Description
GET /alerts	Retrieve all alerts.

Operation	Description
POST /alerts	Create a new alert with specified values.
DELETE /alerts/{id}	Delete a specific alert.
GET /alerts/{id}	Retrieve a specific alert.
PATCH /alerts/{id}	Apply updates to a specific alert.
GET /alerts/{id}/applications	Retrieve all applications that have a specific alert assigned.
POST /alerts/{id}/applications	Assign and unassign a specific alert to applications.
DELETE /alerts/{id}/applications/{child-id}	Unassign an application from a specific alert.
POST /alerts/{id}/applications/{child-id}	Assign an application to a specific alert.
GET /alerts/{id}/devicegroups	Retrieve all device groups that have a specific alert assigned.
POST /alerts/{id}/devicegroups	Assign and unassign a specific alert to device groups.
DELETE /alerts/{id}/devicegroups/{child-id}	Unassign a device group from a specific alert.
POST /alerts/{id}/devicegroups/{child-id}	Assign a device group to a specific alert.
GET /alerts/{id}/devices	Retrieve all devices that have a specific alert assigned.
POST /alerts/{id}/devices	Assign and unassign a specific alert to devices.
DELETE /alerts/{id}/devices/{child-id}	Unassign a device from a specific alert.
POST /alerts/{id}/devices/{child-id}	Assign a device to a specific alert.
GET /alerts/{id}/emailgroups	Retrieve all email groups that have a specific alert assigned.
POST /alerts/{id}/emailgroups	Assign and unassign a specific alert to email groups.
DELETE /alerts/{id}/emailgroups/{child-id}	Unassign a email group from a specific alert.
POST /alerts/{id}/emailgroups/{child-id}	Assign a email group to a specific alert.
GET /alerts/{id}/exclusionintervals	Retrieve all exclustion intervals that have a specific alert assigned.
POST /alerts/{id}/exclusionintervals	Assign and unassign a specific alert to exclustion intervals.
DELETE /alerts/{id}/exclusionintervals/{child-id}	Unassign an exclusion interval from a specific alert.
POST /alerts/{id}/exclusionintervals/{child-id}	Assign an exclusion interval to a specific alert.
GET /alerts/{id}/networks	Retrieve all networks that have a specific alert assigned.
POST /alerts/{id}/networks	Assign and unassign a specific alert to networks.
DELETE /alerts/{id}/networks/{child-id}	Unassign a network from a specific alert.
POST /alerts/{id}/networks/{child-id}	Assign a network to a specific alert.
GET /alerts/{id}/stats	Retrieve all additional statistics for a specific alert.

Operation details

`GET /alerts`

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "apply_all": true,
    "author": "string",
    "categories": [
        "string"
    ],
    "cc": [],
    "description": "string",
    "disabled": true,
    "field_name": "string",
    "field_name2": "string",
    "field_op": "string",
    "id": 0,
    "interval_length": 0,
    "mod_time": 0,
    "name": "string",
    "notify_snmp": true,
    "object_type": "string",
    "operand": "string",
    "operator": "string",
    "param": {},
    "param2": {},
    "protocols": [
        "string"
    ],
    "refire_interval": 0,
    "severity": 0,
    "stat_name": "string",
    "type": "string",
    "units": "string"
}
```

`POST /alerts`

Specify the following parameters.

`body:` ***Object***

Apply the specified property values to the new alert.

`description:` ***String***

An optional description for the alert.

`notify_snmp:` ***Boolean***

(Optional) Indicates whether to send an SNMP trap when an alert is generated.

`field_op:` ***String***

The type of comparison between the field_name and field_name2 fields when applying a ratio. Only applicable to threshold alerts.

The following values are valid:

- `/`
- `null`

`stat_name:` ***String***

The statistic name for the alert. Only applicable to threshold alerts.

`disabled:` ***Boolean***

(Optional) Indicates whether the alert is disabled.

`operator:` ***String***

The logical operator applied when comparing the value of the operand field to alert conditions. Only applicable to threshold alerts.

The following values are valid:

- `==`
- `>`
- `<`
- `>=`
- `<=`

`operand:` ***String***

The value to compare against alert conditions. The compare method is specified by the value of the operator field. Only applicable to threshold alerts.

`field_name:` ***String***

The name of the monitored metric. Only applicable to threshold alerts.

`name:` ***String***

The unique, friendly name for the alert.

`cc:` ***Array of Strings***

The list of email addresses, not included in an email group, to receive notifications.

`apply_all:` ***Boolean***

Indicates whether the alert is assigned to all available data sources.

`severity:` ***Number***

(Optional) The severity level of the alert, which is displayed in the Alert History, email notifications, and SNMP traps. Severity levels 0-2 require immediate attention. Severity levels are described in the REST API Guide.

`author:` ***String***

The name of the user that created the alert.

`param:` ***Object***

The first alert parameter, which is either a key pattern or a data point. Only applicable to threshold alerts.

`interval_length:` ***Number***

The length of the alert interval, expressed in seconds. Only applicable to threshold alerts.

The following values are valid:

- `30`
- `60`
- `120`
- `300`
- `600`
- `900`
- `1200`
- `1800`

`param2:` ***Object***

The second alert parameter, which is either a key pattern or a data point. Only applicable to threshold alerts.

`units:` ***String***

The interval in which to evaluate the alert condition. Only applicable to threshold alerts.

The following values are valid:

- `none`
- `period`
- `1 sec`
- `1 min`
- `1 hr`

`field_name2:` ***String***

The second monitored metric when applying a ratio. Only applicable to threshold alerts.

`refire_interval:` ***Number***

(Optional) The time interval in which alert conditions are monitored, expressed in seconds.

The following values are valid:

- `300`
- `600`
- `900`
- `1800`
- `3600`
- `7200`
- `14400`

`type:` ***String***

The type of alert.

The following values are valid:

- `threshold`

`object_type:` ***String***

The type of metric source monitored by the alert configuration. Only applicable to detection alerts.

The following values are valid:

- `application`
- `device`

`protocols:` ***Array of Strings***

(Optional) The list of monitored protocols. Only applicable to detection alerts.

`categories:` ***Array of Strings***

(Optional) The list of one or more detection categories. An alert is generated only if a detection is identified in the specified categories. Only applicable to detection alerts.

Specify the body parameter in the following JSON format.

```
{
    "apply_all": true,
    "author": "string",
    "categories": [
        "string"
    ],
    "cc": [],
    "description": "string",
    "disabled": true,
    "field_name": "string",
    "field_name2": "string",
```

```
    "field_op": "string",
    "interval_length": 0,
    "name": "string",
    "notify_snmp": true,
    "object_type": "string",
    "operand": "string",
    "operator": "string",
    "param": {},
    "param2": {},
    "protocols": [
        "string"
    ],
    "refire_interval": 0,
    "severity": 0,
    "stat_name": "string",
    "type": "string",
    "units": "string"
}
```

`GET /alerts/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the alert.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "apply_all": true,
    "author": "string",
    "categories": [
        "string"
    ],
    "cc": [],
    "description": "string",
    "disabled": true,
    "field_name": "string",
    "field_name2": "string",
    "field_op": "string",
    "id": 0,
    "interval_length": 0,
    "mod_time": 0,
    "name": "string",
    "notify_snmp": true,
    "object_type": "string",
    "operand": "string",
    "operator": "string",
    "param": {},
    "param2": {},
    "protocols": [
        "string"
    ],
    "refire_interval": 0,
    "severity": 0,
    "stat_name": "string",
    "type": "string",
    "units": "string"
}
```

`DELETE /alerts/{id}`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the alert.

`PATCH /alerts/{id}`

Specify the following parameters.

`body:` ***Object***
Apply the specified property value updates to the alert.

`id:` ***Number***
The unique identifier for the alert.

`GET /alerts/{id}/stats`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the alert.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "alert_id": 0,
    "field_name": "string",
    "id": 0,
    "param": "string",
    "stat_name": "string"
}
```

`GET /alerts/{id}/devicegroups`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the alert.

`POST /alerts/{id}/devicegroups`

Specify the following parameters.

`body:` ***Object***
The list of unique identifiers for device groups that is assigned and unassigned to the alert.

`assign:` ***Array of Numbers***
IDs of resources to assign

`unassign:` ***Array of Numbers***
IDs of resources to unassign

Specify the body parameter in the following JSON format.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Number***
The unique identifier for the alert.

`POST /alerts/{id}/devicegroups/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the device group.
`id:` ***Number***
The unique identifier for the alert.

`DELETE /alerts/{id}/devicegroups/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the device group.
`id:` ***Number***
The unique identifier for the alert.

`GET /alerts/{id}/emailgroups`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the alert.

`POST /alerts/{id}/emailgroups`

Specify the following parameters.

`body:` ***Object***
The list of unique identifiers for email groups that is assigned and unassigned to the alert.
`assign:` ***Array of Numbers***
IDs of resources to assign
`unassign:` ***Array of Numbers***
IDs of resources to unassign
Specify the body parameter in the following JSON format.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Number***
The unique identifier for the alert.

`POST /alerts/{id}/emailgroups/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the email group.

`id:` ***Number***
The unique identifier for the alert.

`DELETE /alerts/{id}/emailgroups/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the email group.
`id:` ***Number***
The unique identifier for the alert.

`GET /alerts/{id}/exclusionintervals`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the alert.

`POST /alerts/{id}/exclusionintervals`

Specify the following parameters.

`body:` ***Object***
The list of unique identifiers for exclusion intervals that is assigned and unassigned to the alert.
`assign:` ***Array of Numbers***
IDs of resources to assign
`unassign:` ***Array of Numbers***
IDs of resources to unassign

Specify the body parameter in the following JSON format.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Number***
The unique identifier for the alert.

`POST /alerts/{id}/exclusionintervals/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the exclusion interval.
`id:` ***Number***
The unique identifier for the alert.

`DELETE /alerts/{id}/exclusionintervals/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the exclusion interval.

`id:` ***Number***
The unique identifier for the alert.

`GET /alerts/{id}/devices`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the alert.

`POST /alerts/{id}/devices`

Specify the following parameters.

`body:` ***Object***
The list of unique identifiers for devices that is assigned and unassigned to the alert.
`assign:` ***Array of Numbers***
IDs of resources to assign
`unassign:` ***Array of Numbers***
IDs of resources to unassign

Specify the body parameter in the following JSON format.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Number***
The unique identifier for the alert.

`POST /alerts/{id}/devices/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the device.
`id:` ***Number***
The unique identifier for the alert.

`DELETE /alerts/{id}/devices/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the device.
`id:` ***Number***
The unique identifier for the alert.

`GET /alerts/{id}/networks`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the alert.

`POST /alerts/{id}/networks`

Specify the following parameters.

`body:` ***Object***
The list of unique identifiers for networks that is assigned and unassigned to the alert.
`assign:` ***Array of Numbers***
IDs of resources to assign
`unassign:` ***Array of Numbers***
IDs of resources to unassign

Specify the body parameter in the following JSON format.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Number***
The unique identifier for the alert.

`POST /alerts/{id}/networks/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the network.
`id:` ***Number***
The unique identifier for the alert.

`DELETE /alerts/{id}/networks/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the network.
`id:` ***Number***
The unique identifier for the alert.

`GET /alerts/{id}/applications`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the alert.

`POST /alerts/{id}/applications`

Specify the following parameters.

`body:` ***Object***
The list of unique identifiers for applications that is assigned and unassigned to the alert.
`assign:` ***Array of Numbers***
IDs of resources to assign
`unassign:` ***Array of Numbers***
IDs of resources to unassign

Specify the body parameter in the following JSON format.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Number***

The unique identifier for the alert.

`POST /alerts/{id}/applications/{child-id}`

Specify the following parameters.

`child-id:` ***Number***

The unique identifier for the application.

`id:` ***Number***

The unique identifier for the alert.

`DELETE /alerts/{id}/applications/{child-id}`

Specify the following parameters.

`child-id:` ***Number***

The unique identifier for the application.

`id:` ***Number***

The unique identifier for the alert.

Analysis Priority

The ExtraHop system analyzes and classifies traffic for every device it discovers. Your license reserves capacity for the ExtraHop system to collect metrics for high value devices. This capacity is associated with two analysis levels: Advanced Analysis and Standard Analysis.

You can specify which devices receive Advanced Analysis and Standard Analysis levels by configuring analysis priority rules. Analysis priorities help inform the ExtraHop system about which devices are important in your environment. A third analysis level, Discovery Mode, is available for devices that are not in Advanced or Standard Analysis.

Note: By default, each sensor manages its own analysis priorities. If the sensor is connected to a console, you can centrally manage these shared system settings from the console.

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /analysispriority/config/{sensor_id}	Retrieve the analysis priority rules for a specific sensor.
PUT /analysispriority/config/{sensor_id}	Replace the analysis priority rules for a specific sensor.
GET /analysispriority/{sensor_id}/manager	Retrieve the system that is configured to manage the analysis priority rules for the sensor.
PATCH /analysispriority/{sensor_id}/manager	Update the system that manages analysis priority rules for a specific sensor.

Operation details

`GET /analysispriority/{appliance_id}/manager`

Specify the following parameters.

`appliance_id:` ***Number***
The identifier for the local sensor. This value must be set to 0.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "manager": {}
}
```

`GET /analysispriority/config/{appliance_id}`

Specify the following parameters.

`appliance_id:` ***Number***
The identifier for a sensor. Set this value to 0 if calling on a sensor.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "advanced_rules": [],
    "autofill_advanced": true,
    "autofill_standard": true,
    "is_in_effect": true,
    "standard_rules": []
}
```

`PUT /analysispriority/config/{appliance_id}`

Specify the following parameters.

`body:` ***Object***
The properties of the priority analysis rules.

`autofill_advanced:` ***Boolean***
Indicates whether to automatically place devices in Advanced Analysis until capacity is reached. Devices in the advanced_rules list are prioritized, followed by devices in the standard_rules list, and then by the discovery time for the device. The capacity for Advanced Analysis is determined by the ExtraHop system license.

`advanced_rules:` ***Array of Objects***
(Optional) The Advanced Analysis priority rules for a device group.

`type:` ***String***
The type of group the analysis priority rules apply to.

The following values are valid:

- `device_group`

`object_id:` ***Number***
The unique identifier for the group.

`description:` ***String***
(Optional) The description for analysis priority rules.

`autofill_standard:` ***Boolean***

Indicates whether to automatically place devices in Standard Analysis until total capacity is reached. Devices in the standard_rules list are prioritized, followed by the discovery time for the device. The total capacity is determined by the ExtraHop system license.

`standard_rules:` ***Array of Objects***

(Optional) The Standard Analysis priority rules for a device group.

`type:` ***String***

The type of group the analysis priority rules apply to.

The following values are valid:

- `device_group`

`object_id:` ***Number***

The unique identifier for the group.

`description:` ***String***

(Optional) The description for analysis priority rules.

Specify the body parameter in the following JSON format.

```
{
    "advanced_rules": {
        "type": "string",
        "object_id": 0,
        "description": "string"
    },
    "autofill_advanced": true,
    "autofill_standard": true,
    "standard_rules": {
        "type": "string",
        "object_id": 0,
        "description": "string"
    }
}
```

`appliance_id:` ***Number***

The identifier for a sensor. Set this value to 0 if calling on a sensor.

`PATCH /analysispriority/{appliance_id}/manager`

Specify the following parameters.

`body:` ***Object***

The ID of the sensor or console that will manage analysis priority rules for the local sensor. Set this value to 0 to restore management to the local sensor.

`manager:` ***Number***

The unique identifier for the managing sensor or console.

Specify the body parameter in the following JSON format.

```
{
    "manager": 0
}
```

`appliance_id:` ***Number***

The identifier for the local sensor. This value must be set to 0.

Appliance

The ExtraHop system consists of a network of connected appliances that perform tasks such as monitoring traffic, analyzing data, storing data, and identifying detections.

You can retrieve information about ExtraHop appliances connected to the local appliance and establish new connections to remote ExtraHop appliances.

Note: You can only establish a connection to a remote ExtraHop appliance that is licensed for the same edition as the local ExtraHop appliance.

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /appliances	Retrieve all remote ExtraHop appliances connected to the local appliance.
GET /appliances/{id}	Retrieve a specific remote ExtraHop appliance connected to the local appliance.
GET /appliances/firmware/next	Retrieve firmware versions that remote ExtraHop systems can be upgraded to.
POST /appliances/firmware/upgrade	Upgrade firmware on remote ExtraHop systems connected to the local system. Firmware images are downloaded from ExtraHop Cloud Services.

Operation details

`GET /appliances`

There are no parameters for this operation.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "add_time": 0,
    "advanced_analysis_capacity": 0,
    "analysis_levels_managed": true,
    "connection_type": "string",
    "data_access": true,
    "display_name": "string",
    "fingerprint": "string",
    "firmware_version": "string",
    "hostname": "string",
    "id": 0,
    "license_platform": "string",
    "license_status": "string",
    "licensed_features": {},
    "licensed_modules": [
        "string"
    ],
    "managed_by_local": true,
    "manages_local": true,
    "nickname": "string",
    "platform": "string",
    "status_message": "string",
    "sync_time": 0,
    "total_capacity": 0,
    "uuid": "string"
```

```
}
```

`GET /appliances/{id}`

Specify the following parameters.

`id:` ***Number***

Specify the unique identifier for the remote appliance.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "add_time": 0,
    "advanced_analysis_capacity": 0,
    "analysis_levels_managed": true,
    "connection_type": "string",
    "data_access": true,
    "display_name": "string",
    "fingerprint": "string",
    "firmware_version": "string",
    "hostname": "string",
    "id": 0,
    "license_platform": "string",
    "license_status": "string",
    "licensed_features": {},
    "licensed_modules": [
        "string"
    ],
    "managed_by_local": true,
    "manages_local": true,
    "nickname": "string",
    "platform": "string",
    "status_message": "string",
    "sync_time": 0,
    "total_capacity": 0,
    "uuid": "string"
}
```

`GET /appliances/{ids_id}/association`

Specify the following parameters.

`ids_id:` ***Number***

Specify the ID of the IDS sensor.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "associated_sensor_id": 0
}
```

`POST /appliances/{ids_id}/association`

Specify the following parameters.

`ids_id:` ***Number***

Specify the ID of the IDS sensor.

`body:` ***Object***

Specify the ID of the packet sensor.

`associated_sensor_id:` ***Number***

The ID of the packet sensor.

Specify the body parameter in the following JSON format.

```
{
    "associated_sensor_id": 0
}
```

`GET /appliances/firmware/next`

Specify the following parameters.

`ids:` ***String***

(Optional) A CSV list of unique identifiers for the remote appliances. If this parameter is specified, the operation returns firmware versions that any of the specified remote appliances can be upgraded to. If this parameter is not specified, the operation returns firmware versions that any remote appliance can be upgraded to.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "release": "string",
    "versions": []
}
```

`POST /appliances/firmware/upgrade`

Specify the following parameters.

`body:` ***Object***

The firmware upgrade options.

`version:` ***String***

The firmware version to upgrade appliances to. You can retrieve a list of valid versions with the GET /api/v1/appliances/firmware/next operation.

`system_ids:` ***Array of Numbers***

A list of unique identifiers for the remote appliances. You can retrieve appliance IDs with the GET /api/v1/appliances operation; appliance IDs are returned in the id fields of the response.

Specify the body parameter in the following JSON format.

```
{
    "system_ids": [],
    "version": "string"
}
```

Application

Applications are user-defined groups that collect metrics identified through triggers across multiple types of traffic. The default All Activity application contains all collected metrics.

The following table displays all of the operations you can perform on the application resource:

Operation	Description
GET /applications	Retrieve all applications that were active within a specific timeframe.
POST /applications	Create a new application.
GET /applications/{id}	Retreive a specific application.
PATCH /applications/{id}	Update a specific application.
GET /applications/{id}/activity	Retrieve all activity for a specific application.
GET /applications/{id}/alerts	Retrieve all alerts that are assigned to a specific application.
POST /applications/{id}/alerts	Assign and unassign alerts to a specific application.
DELETE /applications/{id}/alerts/{child-id}	Unassign an alert from a specific application.
POST /applications/{id}/alerts/{child-id}	Assign an alert to a specific application.
GET /applications/{id}/dashboards	Retrieve all dashboards related to a specific application.

Operation details

`GET /applications/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the application.

`include_criteria:` ***Boolean***

(Optional) Indicates whether to include the criteria associated with the application in the response.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "criteria": [],
    "description": "string",
    "discovery_id": "string",
    "display_name": "string",
    "extrahop_id": "string",
    "id": 0,
    "mod_time": 0,
    "node_id": 0,
    "user_mod_time": 0
}
```

`POST /applications`

Specify the following parameters.

`body:` ***Object***

The properties of the application.

`node_id:` ***Number***

(Optional) The unique identifier for the sensor that this application is associated with. The identifier can be retrieved through the GET /appliances operation. This field is valid only on a console.

`discovery_id:` ***String***

The unique identifier for the application, which is displayed on the application page in the ExtraHop system.

`display_name:` ***String***

The friendly name for the application.

`description:` ***String***

(Optional) An optional description for the application.

`criteria:` ***Array of Objects***

(Optional) An array of protocol and source criteria associated with the application. The contents of this array are defined in the 'criteria' section below.

`protocol_default:` ***String***

The default protocols monitored by the application. Supported values are 'any' and 'none'.

`sources:` ***Array of Objects***

An array containing one or more metric sources associated with the application. The application only collects metrics from the specified sources. The contents of this array are defined in the 'source' section below.

`type:` ***String***

The type of metric source associated with the application. Supported source type values are 'device' and 'device_group'.

`id:` ***Number***

The unique identifier for the device or device group associated with the application.

`protocols:` ***Object***

(Optional) The list of one or more protocol and role mappings associated with the application. The application only collects metrics from the specified protocols. The format of each protocol is {'protocol':'role'}. Example: {'http': 'server'}. Supported role values are 'client', 'server', 'any', or 'none'.

Specify the body parameter in the following JSON format.

```
{
    "criteria": {
        "protocol_default": "string",
        "sources": {
            "type": "string",
            "id": 0
        },
        "protocols": {}
    },
    "description": "string",
    "discovery_id": "string",
    "display_name": "string",
    "node_id": 0
}
```

`PATCH /applications/{id}`

Specify the following parameters.

`body:` ***Object***

Apply the specified property updates to the application.

`id:` ***Number***

The unique identifier for the application.

`GET /applications`

Specify the following parameters.

`active_from:` ***Number***

(Optional) Return only applications that are active after the specified time. Positive values specify the time in milliseconds since the epoch. Negative values specify the time in milliseconds before the current time.

`active_until:` ***Number***

(Optional) Return only applications that are active before the specified time. Positive values specify the time in milliseconds since the epoch. Negative values specify the time in milliseconds before the current time.

`limit:` ***Number***

(Optional) Limit the number of applications that are returned to the specified maximum number.

`offset:` ***Number***

(Optional) Skip the first n application results. This parameter is often combined with the limit parameter.

`search_type:` ***String***

The object type to search for.

The following values are valid:

- `any`
- `name`
- `node`
- `discovery_id`
- `extrahop-id`

`value:` ***String***

(Optional) The search criteria. Add a forward slash before and after the criteria to apply RegEx matching.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "criteria": [],
    "description": "string",
    "discovery_id": "string",
    "display_name": "string",
    "extrahop_id": "string",
    "id": 0,
    "mod_time": 0,
    "node_id": 0,
    "user_mod_time": 0
}
```

`GET /applications/{id}/activity`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the application.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "application_id": 0,
    "from_time": 0,
    "id": 0,
    "mod_time": 0,
    "stat_name": "string",
    "until_time": 0
}
```

`GET /applications/{id}/alerts`

Specify the following parameters.

`id:` ***Number***
Retrieve the unique identifier for the application.

`direct_assignments_only:` ***Boolean***
(Optional) Indicates whether results are restricted to alerts that are directly assigned to the application.

`POST /applications/{id}/alerts`

Specify the following parameters.

`body:` ***Object***
Assign or unassign the specified list of unique identifiers for alerts.

`assign:` ***Array of Numbers***
IDs of resources to assign

`unassign:` ***Array of Numbers***
IDs of resources to unassign

Specify the body parameter in the following JSON format.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Number***
Provide a unique identifier for the application.

`POST /applications/{id}/alerts/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the alert.

`id:` ***Number***
The unique identifier for the application.

`DELETE /applications/{id}/alerts/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the alert.

`id:` ***Number***
The unique identifier for the application.

`GET /applications/{id}/dashboards`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the application.

Audit log

The audit log displays a record of all recorded system administration and configuration activity, such as the time of the activity, the user who performed the activity, the operation, operation details, and system component..

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /auditlog	Retrieve all audit log messages.

Operation details

`GET /auditlog`

Specify the following parameters.

`limit:` ***Number***
(Optional) The maximum number of log messages to return.

`offset:` ***Number***
(Optional) The number of log messages to skip in the results. Returns log messages starting from the offset value.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "body": {},
    "id": 0,
    "occur_time": 0,
    "time": 0
}
```

Bundle

Bundles are JSON-formatted documents that contain information about selected system configuration, such as triggers, dashboards, applications, or alerts.

You can create a bundle and then transfer those configurations to another ExtraHop system, or save the bundle as a backup. Bundles can also be downloaded from ExtraHop Solution Bundles and applied through the REST API. For more information, see Bundles.

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /bundles	Retrieve metadata about all bundles on the ExtraHop system.
POST /bundles	Upload a new bundle to the ExtraHop system.
DELETE /bundles/{id}	Delete a specific bundle.
GET /bundles/{id}	Retrieve a specific bundle export.
POST /bundles/{id}/apply	Apply a saved bundle to the ExtraHop system.

Operation details

`GET /bundles`

There are no parameters for this operation.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "built_in": true,
    "created_time": 0,
    "description": "string",
    "id": 0,
    "mod_time": 0,
    "name": "string"
}
```

`POST /bundles`

Specify the following parameters.

`body:` ***String***

A JSON formatted bundle export.

`name:` ***String***

The friendly name for the bundle.

`description:` ***String***

(Optional) An optional description for the bundle.

Specify the body parameter in the following JSON format.

```
{
    "description": "string",
    "name": "string"
}
```

`GET /bundles/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the bundle.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "built_in": true,
```

```
    "created_time": 0,
    "description": "string",
    "id": 0,
    "mod_time": 0,
    "name": "string"
}
```

`DELETE /bundles/{id}`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the bundle.

`POST /bundles/{id}/apply`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the bundle.

`body:` ***Object***
The configuration options for applying the bundle.

`policy:` ***String***
Indicates whether conflicting objects should be overwritten or skipped.

The following values are valid:

- `overwrite`
- `skip`

`include_assignments:` ***Boolean***
Indicates whether object assignments should be restored with the bundle.

`node_ids:` ***Array of Numbers***
A list of unique identifiers for the sensors on which to apply the bundle. This field is valid only on a console.

Specify the body parameter in the following JSON format.

```
{
    "include_assignments": true,
    "node_ids": [],
    "policy": "string"
}
```

Dashboards

Dashboards are built-in or customized views of your ExtraHop metrics information. For more information, see Dashboards.

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /dashboards	Retrieve all dashboards.
DELETE /dashboards/{id}	Delete a specific dashboard.
GET /dashboards/{id}	Retrieve a specific dashboard.

Operation	Description
PATCH /dashboards/{id}	Update ownership of a specific dashboard.
GET /dashboards/{id}/reports	Retrieve dashboard reports that contain a specific dashboard. **Note:** This operation is only available from a console.
GET /dashboards/{id}/sharing	Retrieve the users and their sharing permissions for a specific dashboard.
PATCH /dashboards/{id}/sharing	Update the users and their sharing permissions for a specific dashboard.
PUT /dashboards/{id}/sharing	Replace the users and their sharing permissions for a specific dashboard.

Operation details

`GET /dashboards`

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "author": "string",
    "comment": "string",
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "owner": "string",
    "rights": [
        "string"
    ],
    "short_code": "string",
    "type": "string"
}
```

`GET /dashboards/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the dashboard.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "author": "string",
    "comment": "string",
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "owner": "string",
    "rights": [
        "string"
    ],
    "short_code": "string",
    "type": "string"
}
```

`DELETE /dashboards/{id}`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the dashboard.

`PATCH /dashboards/{id}`

Specify the following parameters.

`body:` ***Object***
The username of the dashboard owner.
`id:` ***Number***
The unique identifier for the dashboard.

`GET /dashboards/{id}/sharing`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the dashboard.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "anyone": "string",
    "groups": {},
    "users": {}
}
```

`PUT /dashboards/{id}/sharing`

Specify the following parameters.

`body:` ***Object***
The users and their permission levels.
`id:` ***Number***
The unique identifier for the dashboard.

`PATCH /dashboards/{id}/sharing`

Specify the following parameters.

`body:` ***Object***
The users and their permission levels.
`id:` ***Number***
The unique identifier for the dashboard.

`GET /dashboards/{id}/reports`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the dashboard.

Detections

The Detections class enables you to retrieve detections that have been identified by the ExtraHop system.

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /detections	Retrieve all detections.
GET /detections/formats	Retrieve all detection types.
POST /detections/formats	Create a new custom detection type.
DELETE /detections/formats/{id}	Delete a specific custom detection type.
PATCH /detections/formats/{id}	Update a specific custom detection type.
GET /detections/rules/hiding	Retrieve all tuning rules.
POST /detections/rules/hiding	Create a tuning rule.
DELETE /detections/rules/hiding/{id}	Delete a tuning rule.
PATCH /detections/rules/hiding/{id}	Update a tuning rule.
POST /detections/search	Retrieve detections that match the specified search criteria.
PATCH /detections/tickets	Update a ticket associated with detections.
GET /detections/{id}	Retrieve a specific detection.
PATCH /detections/{id}	Update a detection.
DELETE /detections/{id}/notes	Delete the notes for a given detection.
GET /detections/{id}/notes	Retrieve the notes for a given detection.
PUT /detections/{id}/notes	Create or replace notes for a given detection.
GET /detections/{id}/related	Retrieve all detections related to a specific detection.

Operation details

`GET /detections/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the detection.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "appliance_id": 0,
    "assignee": "string",
    "categories": [
        "string"
    ],
    "description": "string",
    "end_time": 0,
    "id": 0,
```

```
    "is_user_created": true,
    "mitre_tactics": [],
    "mitre_techniques": [],
    "mod_time": 0,
    "participants": [],
    "properties": {},
    "recommended": true,
    "recommended_factors": [],
    "resolution": "string",
    "risk_score": 0,
    "start_time": 0,
    "status": "string",
    "ticket_id": "string",
    "ticket_url": "string",
    "title": "string",
    "type": "string",
    "update_time": 0
}
```

`GET /detections`

Specify the following parameters.

`limit:` ***Number***

(Optional) Limit the number of detections returned to the specified maximum number. A random selection of detections is returned.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "appliance_id": 0,
    "assignee": "string",
    "categories": [
        "string"
    ],
    "description": "string",
    "end_time": 0,
    "id": 0,
    "is_user_created": true,
    "mitre_tactics": [],
    "mitre_techniques": [],
    "mod_time": 0,
    "participants": [],
    "properties": {},
    "recommended": true,
    "recommended_factors": [],
    "resolution": "string",
    "risk_score": 0,
    "start_time": 0,
    "status": "string",
    "ticket_id": "string",
    "ticket_url": "string",
    "title": "string",
    "type": "string",
    "update_time": 0
}
```

`POST /detections/search`

Specify the following parameters.

`body:` ***Object***

The detection search parameters.

`filter:` ***Object***

Detection-specific filters.

`category:` ***String***

Deprecated. Replaced by the categories field.

`categories:` ***Array of Strings***

Return detections from the specified categories.

`assignee:` ***Array of Strings***

Returns detections assigned to the specified user. Specify ".none" to search for unassigned detections or specify ".me" to search for detections assigned to the authenticated user.

`ticket_id:` ***Array of Strings***

Returns detections that are associated with the specified tickets. Specify ".none" to search for detections that are not associated with tickets.

`status:` ***Array of Strings***

Returns detections for tickets with the specified status. Specify ".none" to search for detections without a ticket status.

The following values are valid:

- `new`
- `in_progress`
- `closed`
- `acknowledged`

`resolution:` ***Array of Strings***

Returns detections for tickets with the specified resolution. Specify ".none" to search for detections without resolutions.

The following values are valid:

- `action_taken`
- `no_action_taken`

`types:` ***Array of Strings***

Returns detections with the specified types.

`risk_score_min:` ***Number***

Returns detections with risk scores greater than or equal to the specified value.

`recommended:` ***Boolean***

Returns detections recommended for triage. This field is valid only on a console.

`from:` ***Number***

Returns detections that occurred after the specified date, expressed in milliseconds since the epoch. Detections that started before the specified date are returned if the detection was ongoing at that time.

`limit:` ***Number***

Returns no more than the specified number of detections.

`offset:` ***Number***

The number of detections to skip for pagination.

`sort:` ***Array of Objects***

Sorts returned detections by the specified fields. By default, detections are sorted by most recent update time and then ID in ascending order.

`direction:` ***String***

The order in which returned detections are sorted.

The following values are valid:

- `asc`
- `desc`

`field:` ***String***

The field to sort detections by.

`until:` ***Number***

Return detections that ended before the specified date, expressed in milliseconds since the epoch.

`update_time:` ***Number***

Returns detections related to events that occurred after the specified date, expressed in milliseconds since the epoch. Note that ExtraHop Machine Learning Services analyze historical data to generate detections, and so there is a time delay between when the events that cause those detections occur and when the detections are generated. If you search for detections in the same update_time window multiple times, the later search might return detections that were not returned by the earlier search.

`mod_time:` ***Number***

Returns detections that were updated after the specified date, expressed in milliseconds since the epoch.

`id_only:` ***Boolean***

(Optional) Returns only the IDs of the detections.

Specify the body parameter in the following JSON format.

```
{
    "filter": {
        "category": "string",
        "categories": [],
        "assignee": [],
        "ticket_id": [],
        "status": [],
        "resolution": [],
        "types": [],
        "risk_score_min": 0,
        "recommended": true
    },
    "from": 0,
    "id_only": true,
    "limit": 0,
    "mod_time": 0,
    "offset": 0,
    "sort": {
        "direction": "string",
        "field": "string"
    },
    "until": 0,
    "update_time": 0
}
```

`PATCH /detections/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the detection.

`body:` ***Object***

The detection parameters to update.

`ticket_id:` ***String***

The ID of the ticket associated with the detection.

`assignee:` ***String***

The assignee of the detection or the ticket associated with the detection.

`status:` ***String***

The status of the detection or the ticket associated with the detection.

The following values are valid:

- `new`
- `in_progress`
- `closed`
- `acknowledged`

`resolution:` ***String***

The resolution of the detection or the ticket associated with the detection.

The following values are valid:

- `action_taken`
- `no_action_taken`

`participants:` ***Array of Objects***

A list of devices and applications associated with the detection. You can modify specific fields for a participant, but you cannot add new participants to a detection.

`id:` ***Number***

The ID of the participant associated with the detection.

`usernames:` ***Array of Strings***

The usernames associated with the participant through the REST API.

`origins:` ***Array of Strings***

The origin IP addresses associated with the participant through the REST API.

Specify the body parameter in the following JSON format.

```
{
    "assignee": "string",
    "participants": {
        "id": 0,
        "usernames": [],
        "origins": []
    },
    "resolution": "string",
    "status": "string",
    "ticket_id": "string"
}
```

`PATCH /detections/tickets`

Specify the following parameters.

`body:` ***Object***

The detection ticketing values to update.

`ticket_id:` ***String***
The ID of the ticket associated with the detection.

`assignee:` ***String***
The assignee of the ticket associated with the detection.

`status:` ***String***
The status of the ticket associated with the detection.

The following values are valid:

- `new`
- `in_progress`
- `closed`
- `acknowledged`

`resolution:` ***String***
The resolution of the ticket associated with the detection.

The following values are valid:

- `action_taken`
- `no_action_taken`

Specify the body parameter in the following JSON format.

```
{
    "assignee": "string",
    "resolution": "string",
    "status": "string",
    "ticket_id": "string"
}
```

`GET /detections/{id}/related`

Specify the following parameters.

`id:` ***Number***
The ID of the detection to retrieve related detections for.

`from:` ***Number***
Returns detections that occurred after the specified date, expressed in milliseconds since the epoch. Detections that started before the specified date are returned if the detection was ongoing at that time.

`until:` ***Number***
Return detections that ended before the specified date, expressed in milliseconds since the epoch.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "appliance_id": 0,
    "assignee": "string",
    "categories": [
        "string"
    ],
    "description": "string",
    "end_time": 0,
    "id": 0,
    "is_user_created": true,
    "mitre_tactics": [],
    "mitre_techniques": [],
    "mod_time": 0,
```

```
    "participants": [],
    "properties": {},
    "recommended": true,
    "recommended_factors": [],
    "resolution": "string",
    "risk_score": 0,
    "start_time": 0,
    "status": "string",
    "ticket_id": "string",
    "ticket_url": "string",
    "title": "string",
    "type": "string",
    "update_time": 0
}
```

`GET /detections/formats`

There are no parameters for this operation.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "author": "string",
    "categories": [],
    "display_name": "string",
    "is_user_created": true,
    "mitre_categories": [],
    "properties": {},
    "type": "string"
}
```

`POST /detections/formats`

Specify the following parameters.

`body:` ***Object***

The parameters of the detection format.

`type:` ***String***

A string identifier for the detection type. The string can only contain letters, numbers, and underscores. Although detection types are unique across built-in formats, and detection types are unique across custom formats, a built-in and custom format can share the same detection type.

`display_name:` ***String***

The display name of the detection type that appears on the Detections page in the ExtraHop system.

`mitre_categories:` ***Array of Strings***

(Optional) The IDs of the MITRE techniques associated with the detection.

`author:` ***String***

(Optional) The author of the detection format.

`categories:` ***Array of Strings***

(Optional) The list of categories the detection belongs to. For POST and PATCH operations, specify a list with a single string. You cannot specify more than one category for custom detection formats. The "perf" or "sec" category is automatically added to all detection formats.

Specify the body parameter in the following JSON format.

```
{
```

```
    "author": "string",
    "categories": [],
    "display_name": "string",
    "mitre_categories": [],
    "type": "string"
}
```

`DELETE /detections/formats/{id}`

Specify the following parameters.

`id:` ***String***
The string identifier of the detection format.

`PATCH /detections/formats/{id}`

Specify the following parameters.

`id:` ***String***
The string identifier of the detection format.

`body:` ***Object***
The parameters of the detection format.

`GET /detections/rules/hiding`

There are no parameters for this operation.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "author": "string",
    "create_time": 0,
    "description": "string",
    "detection_type": "string",
    "detections_hidden": 0,
    "enabled": true,
    "expiration": 0,
    "hide_past_detections": true,
    "id": 0,
    "offender": {},
    "participants_hidden": 0,
    "properties": [],
    "victim": {}
}
```

`POST /detections/rules/hiding`

Specify the following parameters.

`body:` ***Object***
The tuning rule parameters.

`offender:` ***Object***
The offender that this tuning rule applies to. Specify a detection_hiding_participant object to apply the rule to a specific victim, or specify "Any" to apply the rule to any offender.

`object_type:` ***String***
The type of participant.

The following values are valid:

- `device`
- `device_group`
- `ipaddr`
- `locality_type`
- `network_locality`
- `scanner_service`

`object_id:` ***Number***

The ID for the device, device group, or network locality. This option is valid only if the object_type is "device", "device_group", or "network_locality".

`object_value:` ***Array or String***

The IP address or CIDR block of the participant. You can specify a single address or block in a string or multiple addresses or blocks in an array. This option is valid only if the object_type is "ipaddr".

`object_locality:` ***String***

The network locality type of the participant. Specify either "external" or "internal". This option is valid only if the object_type is "locality_type".

The following values are valid:

- `internal`
- `external`

`object_scanner:` ***Array or String***

The name of an external scanning service. You can specify a single service in a string or multiple values in an array. You can also specify "Any" to select any scanning service. This option is valid only if the object_type is "scanner_service".

`victim:` ***Object***

The victim that this tuning rule applies to. Specify a detection_hiding_participant object to apply the rule to a specific victim, or specify "Any" to apply the rule to any victim.

`object_type:` ***String***

The type of participant.

The following values are valid:

- `device`
- `device_group`
- `ipaddr`
- `locality_type`
- `network_locality`
- `scanner_service`

`object_id:` ***Number***

The ID for the device, device group, or network locality. This option is valid only if the object_type is "device", "device_group", or "network_locality".

`object_value:` ***Array or String***

The IP address or CIDR block of the participant. You can specify a single address or block in a string or multiple addresses or blocks in an array. This option is valid only if the object_type is "ipaddr".

`object_locality:` ***String***

The network locality type of the participant. Specify either "external" or "internal". This option is valid only if the object_type is "locality_type".

The following values are valid:

- `internal`

- `external`

`object_scanner:` ***Array or String***

The name of an external scanning service. You can specify a single service in a string or multiple values in an array. You can also specify "Any" to select any scanning service. This option is valid only if the object_type is "scanner_service".

`expiration:` ***Number***

The time that the tuning rule expires, expressed in milliseconds since the epoch. A value of null or 0 indicates that the rule does not expire.

`description:` ***String***

(Optional) The description of the tuning rule.

`detection_type:` ***String***

The type of detection that this tuning rule applies to. View a list of valid fields for "type" by running the GET /detections/formats operation. Specify "all_performance" or "all_security" to apply the rule to all performance or all security detections.

`properties:` ***Array of Objects***

(Optional) The filter criteria for detection properties.

`property:` ***String***

The name of the property to filter.

`operator:` ***String***

The compare method applied when matching the operand value against the detection property value.

The following values are valid:

- `=`
- `!=`
- `~`
- `!~`
- `in`

`operand:` ***String or Number or Object***

The value that the filter attempts to match. The filter compares the value of the operand to the value of the detection property and applies the compare method specified by the operator parameter. You can specify the operand as a string, integer, or object. For more information, see the REST API Guide.

Specify the body parameter in the following JSON format.

```
{
    "description": "string",
    "detection_type": "string",
    "expiration": 0,
    "offender": {
        "object_type": "string",
        "object_id": 0,
        "object_value": "array",
        "object_locality": "string",
        "object_scanner": "array"
    },
    "properties": {
        "property": "string",
        "operator": "string",
        "operand": "string"
    },
    "victim": {
        "object_type": "string",
```

```
        "object_id": 0,
        "object_value": "array",
        "object_locality": "string",
        "object_scanner": "array"
    }
}
```

`PATCH /detections/rules/hiding/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the tuning rule.

`body:` ***Object***

The tuning rule fields to update.

`enabled:` ***Boolean***

Indicates whether the tuning rule is enabled.

`expiration:` ***Number***

The time that the tuning rule expires, expressed in milliseconds since the epoch. A value of null or 0 indicates that the rule does not expire.

`description:` ***String***

The description of the tuning rule.

`offender:` ***Object***

The offender that this tuning rule applies to. Specify a detection_hiding_participant object to apply the rule to a specific victim, or specify "Any" to apply the rule to any offender.

`object_type:` ***String***

The type of participant.

The following values are valid:

- `device`
- `device_group`
- `ipaddr`
- `locality_type`
- `network_locality`
- `scanner_service`

`object_id:` ***Number***

The ID for the device, device group, or network locality. This option is valid only if the object_type is "device", "device_group", or "network_locality".

`object_value:` ***Array or String***

The IP address or CIDR block of the participant. You can specify a single address or block in a string or multiple addresses or blocks in an array. This option is valid only if the object_type is "ipaddr".

`object_locality:` ***String***

The network locality type of the participant. Specify either "external" or "internal". This option is valid only if the object_type is "locality_type".

The following values are valid:

- `internal`
- `external`

`object_scanner:` ***Array or String***

The name of an external scanning service. You can specify a single service in a string or multiple values in an array. You can also specify "Any" to select any scanning service. This option is valid only if the object_type is "scanner_service".

`victim:` ***Object***

The victim that this tuning rule applies to. Specify a detection_hiding_participant object to apply the rule to a specific victim, or specify "Any" to apply the rule to any victim.

`object_type:` ***String***

The type of participant.

The following values are valid:

- `device`
- `device_group`
- `ipaddr`
- `locality_type`
- `network_locality`
- `scanner_service`

`object_id:` ***Number***

The ID for the device, device group, or network locality. This option is valid only if the object_type is "device", "device_group", or "network_locality".

`object_value:` ***Array or String***

The IP address or CIDR block of the participant. You can specify a single address or block in a string or multiple addresses or blocks in an array. This option is valid only if the object_type is "ipaddr".

`object_locality:` ***String***

The network locality type of the participant. Specify either "external" or "internal". This option is valid only if the object_type is "locality_type".

The following values are valid:

- `internal`
- `external`

`object_scanner:` ***Array or String***

The name of an external scanning service. You can specify a single service in a string or multiple values in an array. You can also specify "Any" to select any scanning service. This option is valid only if the object_type is "scanner_service".

`properties:` ***Array of Objects***

The filter criteria for detection properties.

`property:` ***String***

The name of the property to filter.

`operator:` ***String***

The compare method applied when matching the operand value against the detection property value.

The following values are valid:

- `=`
- `!=`
- `~`
- `!~`
- `in`

`operand:` ***String or Number or Object***

The value that the filter attempts to match. The filter compares the value of the operand to the value of the detection property and applies the compare method specified by the operator parameter. You can specify the operand as a string, integer, or object. For more information, see the REST API Guide.

Specify the body parameter in the following JSON format.

```
{
    "description": "string",
    "enabled": true,
    "expiration": 0,
    "offender": {
        "object_type": "string",
        "object_id": 0,
        "object_value": "array",
        "object_locality": "string",
        "object_scanner": "array"
    },
    "properties": {
        "property": "string",
        "operator": "string",
        "operand": "string"
    },
    "victim": {
        "object_type": "string",
        "object_id": 0,
        "object_value": "array",
        "object_locality": "string",
        "object_scanner": "array"
    }
}
```

`DELETE /detections/rules/hiding/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the tuning rule.

`GET /detections/{id}/notes`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the detection.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "author": "string",
    "note": "string",
    "update_time": 0
}
```

`DELETE /detections/{id}/notes`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the detection.

`PUT /detections/{id}/notes`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the detection.

`body:` ***Object***

The detection note parameters.

Operand values for detection property tuning rules

The `POST /detections/rules/hiding` operation enables you to create tuning rules that filter detections based on detection properties. You can specify filtering criteria for detection properties in objects. Each object should contain a unique value for the `operand` field that is valid for the specified `property` value.

Tip: You can retrieve valid property values through the `GET /detections/formats` operation. See the keys of the `properties` object in the response. In the following example, the `property` value is `s3_bucket`:

```
    "properties": {
      "s3_bucket": {
        "is_optional": true,
        "status": "active",
        "is_tunable": true,
        "data_type": "string"
      }
    }
```

The `is_tunable` field indicates whether you can create a tuning rule based on the property.

`registered_domain_name`

To hide rules by a registered domain name, specify the `property` value as `registered_domain_name` and the `operand` value as a domain name.

The following example rule hides DNS Tunnel detections for `example.com`.

```
{
    "detection_type": "dns_tunnel",
    "expiration": null,
    "offender": "Any",
    "victim": "Any",
    "properties": [
        {
            "operand": "example.com",
            "operator": "=",
            "property": "registered_domain_name"
        }
    ]
}
```

`uris`

To hide rules by a URI, specify the `property` value as `uris` and the `operand` value as a URI.

The following example rule hides SQL Injection (SQLi) Attack detections for `http://example.com/test`.

```
{
    "detection_type": "sqli_attack",
    "expiration": null,
    "offender": "Any",
    "victim": "Any",
    "properties": [
        {
            "operand": "http://example.com/test",
            "operator": "=",
            "property": "uris"
        }
      ]
}
```

`top_level_domain`

To hide rules by a top-level domain name, specify the `property` value as `top_level_domain` and the `operand` value as a top-level domain name.

The following example rule hides Suspicious Top-level Domain detections for the `org` top-level domain.

```
{
    "detection_type": "suspicious_tld",
    "expiration": null,
    "offender": "Any",
    "victim": "Any",
    "properties": [
        {
            "operand": "org",
            "operator": "=",
            "property": "top_level_domain"
        }
    ]
}
```

Search with regular expressions (regex)

For certain `property` values, the string can be in regex syntax. Specify the `operand` value as an object that has a `value` parameter with the regex syntax you want to match and an `is_regex` parameter that is set to `true`. The following rule filters DNS Tunnel detections with domain names that end with `example.com`.

```
{
    "detection_type": "dns_tunnel",
    "expiration": null,
    "offender": "Any",
    "victim": "Any",
    "properties": [
        {
            "operand": {
                "value": ".*?example.com",
                "is_regex": true
            },
            "operator": "=",
            "property": "registered_domain_name"
        }
    ]
```

```
}
```

Disable case sensitivity

By default, searches for string `property` values are case-sensitive. However, you can disable case sensitivity by specifying the operand value as an object that has a `case_sensitive` parameter that is set to `false`.

The following rule hides Hacking Tool Domain Access detections with the ArchStrike hacking tool.

```
{
    "detection_type": "hacking_tools",
    "expiration": null,
    "offender": "Any",
    "victim": "Any",
    "properties": [
        {
            "operand": {
                "value": "archstrike",
                "case_sensitive": false
            },
            "operator": "=",
            "property": "hacking_tool"
        }
    ]
}
```

Detection categories

The categories field is an array returned in responses for `GET /detections` and `POST /detections/search` operations. The following table lists valid entries in the array:

Value	Category
`sec`	Security
`sec.action`	Actions on Objective
`sec.botnet`	Botnet
`sec.caution`	Caution
`sec.command`	Command & Control
`sec.cryptomining`	Cryptomining
`sec.dos`	Denial of Service
`sec.exfil`	Exfiltration
`sec.exploit`	Exploitation
`sec.hardening`	Hardening
`sec.lateral`	Lateral Movement
`sec.ransomware`	Ransomware
`sec.recon`	Reconnaissance
`perf`	Performance
`perf.auth`	Authorization & Access Control
`perf.db`	Database

Value	Category
`perf.network`	Network Infrastructure
`perf.service`	Service Degradation
`perf.storage`	Storage
`perf.virtual`	Desktop & App Virtualization
`perf.web`	Web Application

Device group

Device groups can be either static or dynamic.

A static device group is user-defined; you create a device group and then manually identify and assign each device to that group. A dynamic device group is defined and automatically managed by a set of configured rules.

For example, you can create a device group and then set a rule to classify all devices within a certain IP address range to be added to that group automatically. For more information, see Device Groups.

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /devicegroups	Retrieve all device groups that were active within a specific time period.
POST /devicegroups	Create a new device group.
DELETE /devicegroups/{id}	Delete a device group.
GET /devicegroups/{id}	Retrieve a specific device group.
PATCH /devicegroups/{id}	Update a specific device group.
GET /devicegroups/{id}/alerts	Retrieve all alerts that are assigned to a specific device group.
POST /devicegroups/{id}/alerts	Assign and unassign a specific device group to alerts.
DELETE /devicegroups/{id}/alerts/{child-id}	Unassign an alert from a specific device group.
POST /devicegroups/{id}/alerts/{child-id}	Assign an alert to a specific device group.
GET /devicegroups/{id}/dashboards	Retrieve all dashboards related to a specific device group.
GET /devicegroups/{id}/devices	Retrieve all devices in the device group that are active within a specific time window. **Note:** A device is considered inactive after five minutes of not sending or receiving packets. However, if a device resumes sending or receiving packets after a period of inactivity shorter than five days, the device is considered to have been active continuously, including during the period of inactivity.

Operation	Description
POST /devicegroups/{id}/devices	Assign and unassign a devices to a specific static device group.
DELETE /devicegroups/{id}/devices/{child-id}	Unassign a device from a specific static device group.
POST /devicegroups/{id}/devices/{child-id}	Assign a device to a specific static device group.
GET /devicegroups/{id}/triggers	Retrieve all triggers that are assigned to a specific device group.
POST /devicegroups/{id}/triggers	Assign and unassign a specific device group to triggers.
DELETE /devicegroups/{id}/triggers/{child-id}	Unassign a trigger from a specific device group.
POST /devicegroups/{id}/triggers/{child-id}	Assign a trigger to a specific device group.

Operation details

`GET /devicegroups`

Specify the following parameters.

`since:` ***Number***

(Optional) Only return device groups that were modified after this time, expressed in milliseconds since the epoch.

`all:` ***Boolean***

(Optional) Deprecated. Replaced by the type parameter.

`name:` ***String***

(Optional) The Regex search value to filter the device groups by name.

`type:` ***String***

(Optional) Only return device groups of the specified type.

The following values are valid:

- `user_created`
- `built_in`
- `all`

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "built_in": true,
    "description": "string",
    "dynamic": true,
    "editors": [],
    "field": "string",
    "filter": {},
    "id": 0,
    "include_custom_devices": true,
    "mod_time": 0,
    "name": "string",
    "value": "string"
}
```

`GET /devicegroups/{id}`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the device group.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "built_in": true,
    "description": "string",
    "dynamic": true,
    "editors": [],
    "field": "string",
    "filter": {},
    "id": 0,
    "include_custom_devices": true,
    "mod_time": 0,
    "name": "string",
    "value": "string"
}
```

`POST /devicegroups`

Specify the following parameters.

`body:` ***Object***
Apply the specified property values to the new device group.

`description:` ***String***
An optional description of the device group.

`name:` ***String***
The friendly name for the device group.

`include_custom_devices:` ***Boolean***
(Optional) Deprecated. Replaced by the filter parameter.

`dynamic:` ***Boolean***
(Optional) Indicates whether the device group is dynamic.

`field:` ***String***
Deprecated. Replaced by the filter parameter.

The following values are valid:

- `any`
- `name`
- `ip address`
- `mac address`
- `vendor`
- `type`
- `tag`
- `vlan`
- `activity`
- `node`
- `discover time`

`value:` ***Object***
(Optional) Deprecated. Replaced by the filter parameter.

`filter:` ***Object***

(Optional) Specify the filter criteria for search results.

`field:` ***String***

The name of the field to filter results on. The search compares the contents of the field parameter to the value of the operand parameter.

The following values are valid:

- `name`
- `ipaddr`
- `macaddr`
- `vendor`
- `tag`
- `activity`
- `node`
- `vlan`
- `discover_time`
- `role`
- `dns_name`
- `dhcp_name`
- `netbios_name`
- `cdp_name`
- `custom_name`
- `software`
- `model`
- `is_critical`
- `instance_id`
- `instance_name`
- `instance_type`
- `cloud_account`
- `vpc_id`
- `subnet_id`
- `is_active`
- `network_locality_type`
- `network_locality_id`
- `id`

`operator:` ***String***

The compare method applied when matching the operand value against the field contents. All filter objects require an operator.

The following values are valid:

- `>`
- `<`
- `<=`
- `>=`
- `=`
- `!=`
- `startswith`
- `and`
- `or`
- `not`

- `exists`
- `not_exists`
- `~`
- `!~`

`operand:` ***String or Number or Object***

The value that the query attempts to match. The query compares the value of the operand to the contents of the field parameter and applies the compare method specified by the operator parameter. You can specify the operand as a string, integer, or object. For information about object values, see the REST API Guide.

`rules:` ***Array of Objects***

An array of one or more filter objects, which can be embedded recursively. Only "and", "or", and "not" operators are allowed for this parameter.

`editors:` ***Array of Strings***

(Optional) The list of users that can edit the device group.

Specify the body parameter in the following JSON format.

```
{
    "description": "string",
    "dynamic": true,
    "editors": [],
    "field": "string",
    "filter": {
        "field": "string",
        "operator": "string",
        "operand": "string",
        "rules": []
    },
    "include_custom_devices": true,
    "name": "string",
    "value": "string"
}
```

`DELETE /devicegroups/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the device group.

`PATCH /devicegroups/{id}`

Specify the following parameters.

`body:` ***Object***

Apply the specified property value updates to a specific device group.

`description:` ***String***

An optional description of the device group.

`name:` ***String***

The friendly name for the device group.

`include_custom_devices:` ***Boolean***

(Optional) Deprecated. Replaced by the filter parameter.

`field:` ***String***

Deprecated. Replaced by the filter parameter.

The following values are valid:

- any
- name
- ip address
- mac address
- vendor
- type
- tag
- vlan
- activity
- node
- discover time

`value:` ***Object***

(Optional) Deprecated. Replaced by the filter parameter.

`filter:` ***Object***

(Optional) Specify the filter criteria for search results.

`editors:` ***Array of Strings***

(Optional) The list of users that can edit the device group.

Specify the body parameter in the following JSON format.

```
{
    "description": "string",
    "editors": [],
    "field": "string",
    "filter": {},
    "include_custom_devices": true,
    "name": "string",
    "value": "string"
}
```

`id:` ***Number***

The unique identifier for the device group.

`GET /devicegroups/{id}/alerts`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the device group.

`direct_assignments_only:` ***Boolean***

(Optional) Restrict results to only alerts that are directly assigned to the device group.

`POST /devicegroups/{id}/alerts/{child-id}`

Specify the following parameters.

`child-id:` ***Number***

The unique identifier for the alert.

`id:` ***Number***

The unique identifier for the device group.

`DELETE /devicegroups/{id}/alerts/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the alert.

`id:` ***Number***
The unique identifier for the device group.

`POST /devicegroups/{id}/alerts`

Specify the following parameters.

`body:` ***Object***
The list of unique identifiers for alerts that is assigned and unassigned to the device group.

`assign:` ***Array of Numbers***
IDs of resources to assign

`unassign:` ***Array of Numbers***
IDs of resources to unassign

Specify the body parameter in the following JSON format.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Number***
The unique identifier for the device group.

`GET /devicegroups/{id}/triggers`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the device group.

`direct_assignments_only:` ***Boolean***
(Optional) Restrict results to only triggers that are directly assigned to the device group.

`POST /devicegroups/{id}/triggers/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the trigger.

`id:` ***Number***
The unique identifier for the device group.

`DELETE /devicegroups/{id}/triggers/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the trigger.

`id:` ***Number***
The unique identifier for the device group.

`POST /devicegroups/{id}/triggers`

Specify the following parameters.

`body:` ***Object***
The list of unique identifiers for triggers that is assigned and unassigned to the device group.
`assign:` ***Array of Numbers***
IDs of resources to assign
`unassign:` ***Array of Numbers***
IDs of resources to unassign

Specify the body parameter in the following JSON format.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Number***
The unique identifier for the device group.

`POST /devicegroups/{id}/devices/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for a device.
`id:` ***Number***
The unique identifier for the device group.

`DELETE /devicegroups/{id}/devices/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for a device.
`id:` ***Number***
The unique identifier for the device group.

`POST /devicegroups/{id}/devices`

Specify the following parameters.

`body:` ***Object***
The list of unique identifiers for devices that is assigned and unassigned to the device group.
`assign:` ***Array of Numbers***
IDs of resources to assign
`unassign:` ***Array of Numbers***
IDs of resources to unassign

Specify the body parameter in the following JSON format.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Number***

The unique identifier for the device group.

`GET /devicegroups/{id}/devices`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the device group.

`active_from:` ***Number***

(Optional) The beginning timestamp for the request. Return only devices active after this time. Time is expressed in milliseconds since the epoch. 0 indicates the time of the request. A negative value is evaluated relative to the current time. The default unit for a negative value is milliseconds, but other units can be specified with a unit suffix. See the REST API Guide for supported time units and suffixes.

`active_until:` ***Number***

(Optional) The ending timestamp for the request. Return only device active before this time. Follows the same time value guidelines as the active_from parameter.

`limit:` ***Number***

(Optional) Limit the number of devices returned.

`offset:` ***Number***

(Optional) Skip the first n device results. This parameter is often combined with the limit parameter.

`GET /devicegroups/{id}/dashboards`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the device group.

Device

Devices are objects on your network that have been identified and classified by your ExtraHop system. For more information, see Devices.

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /devices	Retrieve all devices that were active within a specific time period. For more information, see Extract the device list through the REST API. **Note:** A device is considered inactive after five minutes of not sending or receiving packets. However, if a device resumes sending or receiving packets after a period of inactivity shorter than five days, the device is considered to have been active continuously, including during the period of inactivity.
POST /devices/search	Retrieve all devices that match specific criteria. For more information, see Search for a device through the REST API.

Operation	Description
	Note: A device is considered inactive after five minutes of not sending or receiving packets. However, if a device resumes sending or receiving packets after a period of inactivity shorter than five days, the device is considered to have been active continuously, including during the period of inactivity.
GET /devices/{id}	Retrieve a specific device.
PATCH /devices/{id}	Update a specific device.
GET /devices/{id}/activity	Retrieve all activity for a device.
GET /devices/{id}/alerts	Retrieve all alerts that are assigned to a specific device.
POST /devices/{id}/alerts	Assign and unassign a specific device to alerts.
DELETE /devices/{id}/alerts/{child-id}	Unassign an alert from a specific device.
POST /devices/{id}/alerts/{child-id}	Assign an alert to a specific device.
GET /devices/{id}/dashboards	Retrieve all dashboards related to a specific device.
GET /devices/{id}/devicegroups	Retrieve all device groups that are assigned to a specific device.
POST /devices/{id}/devicegroups	Assign and unassign a specific device to device groups.
DELETE /devices/{id}/devicegroups/{child-id}	Unassign a device group from a specific device.
POST /devices/{id}/devicegroups/{child-id}	Assign a device group to a specific device.
GET /devices/{id}/dnsnames	Retrieve all DNS names that are associated with a specific device.
GET /devices/{id}/ipaddrs	Retrieve all IP addresses that were associated with a specific device within a given time period.
GET /devices/{id}/software	Retrieve a list of software running on the specified device.
GET /devices/{id}/tags	Retrieve all tags that are assigned to a specific device.
POST /devices/{id}/tags	Assign and unassign a specific device to tags.
DELETE /devices/{id}/tags/{child-id}	Unassign a tag from a specific device.
POST /devices/{id}/tags/{child-id}	Assign a tag to a specific device.
GET /devices/{id}/triggers	Retrieve all triggers that are assigned to a specific device.
POST /devices/{id}/triggers	Assign and unassign a specific device to triggers.
DELETE /devices/{id}/triggers/{child-id}	Unassign a trigger from a specific device.
POST /devices/{id}/triggers/{child-id}	Assign a trigger to a specific device.

Operation details

```
GET /devices
```

Specify the following parameters.

`active_from:` ***Number***

(Optional) The beginning timestamp for the request. Return only devices active after this time. Time is expressed in milliseconds since the epoch. 0 indicates the time of the request. A negative value is evaluated relative to the current time. The default unit for a negative value is milliseconds, but other units can be specified with a unit suffix. See the REST API Guide for supported time units and suffixes.

`active_until:` ***Number***

(Optional) The ending timestamp for the request. Return only device active before this time. Follows the same time value guidelines as the active_from parameter.

`limit:` ***Number***

(Optional) Limit the number of devices returned to the specified maximum number.

`offset:` ***Number***

(Optional) Skip the first n device results. This parameter is often combined with the limit parameter.

`search_type:` ***String***

Indicates the field to search.

The following values are valid:

- `any`
- `name`
- `discovery_id`
- `ip address`
- `mac address`
- `vendor`
- `type`
- `tag`
- `activity`
- `node`
- `vlan`
- `discover time`

`value:` ***String***

(Optional) Specifies the search criteria.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "activity": [],
    "analysis": "string",
    "analysis_level": 0,
    "auto_role": "string",
    "cdp_name": "string",
    "cloud_account": "string",
    "cloud_instance_description": "string",
    "cloud_instance_id": "string",
    "cloud_instance_name": "string",
    "cloud_instance_type": "string",
    "critical": true,
    "custom_criticality": "string",
    "custom_make": "string",
```

```
    "custom_model": "string",
    "custom_name": "string",
    "custom_type": "string",
    "default_name": "string",
    "description": "string",
    "device_class": "string",
    "dhcp_name": "string",
    "discover_time": 0,
    "discovery_id": "string",
    "display_name": "string",
    "dns_name": "string",
    "extrahop_id": "string",
    "id": 0,
    "ipaddr4": "string",
    "ipaddr6": "string",
    "is_l3": true,
    "last_seen_time": 0,
    "macaddr": "string",
    "mod_time": 0,
    "model": "string",
    "model_override": "string",
    "netbios_name": "string",
    "node_id": 0,
    "on_watchlist": true,
    "parent_id": 0,
    "role": "string",
    "subnet_id": "string",
    "user_mod_time": 0,
    "vendor": "string",
    "vlanid": 0,
    "vpc_id": "string"
}
```


`POST /devices/search`

Specify the following parameters.

`body:` ***Object***

The device criteria.

`active_from:` ***Number***

(Optional) The beginning timestamp for the request. Return only devices active after this time. Time is expressed in milliseconds since the epoch. 0 indicates the time of the request. A negative value is evaluated relative to the current time. The default unit for a negative value is milliseconds, but other units can be specified with a unit suffix. See the REST API Guide for supported time units and suffixes.

`active_until:` ***Number***

(Optional) The ending timestamp for the request. Return only devices active before this time. Follows the same time value guidelines as the active_from parameter.

`limit:` ***Number***

(Optional) Limit the number of devices returned to the specified maximum number.

`offset:` ***Number***

(Optional) Skip the specified number of devices. This parameter is often combined with the limit parameter to paginate result sets.

`filter:` ***Object***

(Optional) Specify the filter criteria for search results.

`field:` ***String***

The name of the field to filter results on. The search compares the contents of the field parameter to the value of the operand parameter.

The following values are valid:

- `name`
- `discovery_id`
- `ipaddr`
- `macaddr`
- `vendor`
- `tag`
- `activity`
- `node`
- `vlan`
- `discover_time`
- `role`
- `dns_name`
- `dhcp_name`
- `netbios_name`
- `cdp_name`
- `custom_name`
- `software`
- `model`
- `is_critical`
- `instance_id`
- `instance_name`
- `instance_type`
- `cloud_account`
- `vpc_id`
- `subnet_id`
- `is_active`
- `analysis`
- `network_locality_type`
- `network_locality_id`
- `id`

`operator:` ***String***

The compare method applied when matching the operand value against the field contents. All filter objects require an operator.

The following values are valid:

- `>`
- `<`
- `<=`
- `>=`
- `=`
- `!=`
- `startswith`
- `and`
- `or`
- `not`

- exists
- not_exists
- ~
- !~
- in
- not_in

`operand:` ***String or Number or Object or Array***

The value that the query attempts to match. The query compares the value of the operand to the contents of the field parameter and applies the compare method specified by the operator parameter. You can specify the operand as a string, integer, or object. For information about object values, see the REST API Guide.

`rules:` ***Array of Objects***

An array of one or more filter objects, which can be embedded recursively. Only "and", "or", and "not" operators are allowed for this parameter.

`result_fields:` ***Array of Strings***

(Optional) Returns the specified fields and the device id. If this option is not specified, all fields are returned.

The following values are valid:

- mod_time
- node_id
- id
- extrahop_id
- discovery_id
- display_name
- description
- user_mod_time
- discover_time
- vlanid
- parent_id
- macaddr
- vendor
- is_l3
- ipaddr4
- ipaddr6
- device_class
- default_name
- custom_name
- cdp_name
- dhcp_name
- netbios_name
- dns_name
- custom_type
- auto_role
- analysis_level
- analysis
- role
- on_watchlist
- last_seen_time
- activity

- model
- model_override
- custom_make
- custom_model
- critical
- custom_criticality
- cloud_instance_id
- cloud_instance_type
- cloud_instance_description
- cloud_instance_name
- cloud_account
- vpc_id
- subnet_id

Specify the body parameter in the following JSON format.

```
{
    "active_from": 0,
    "active_until": 0,
    "filter": {
        "field": "string",
        "operator": "string",
        "operand": "string",
        "rules": []
    },
    "limit": 0,
    "offset": 0,
    "result_fields": []
}
```

`GET /devices/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "activity": [],
    "analysis": "string",
    "analysis_level": 0,
    "auto_role": "string",
    "cdp_name": "string",
    "cloud_account": "string",
    "cloud_instance_description": "string",
    "cloud_instance_id": "string",
    "cloud_instance_name": "string",
    "cloud_instance_type": "string",
    "critical": true,
    "custom_criticality": "string",
    "custom_make": "string",
    "custom_model": "string",
    "custom_name": "string",
    "custom_type": "string",
    "default_name": "string",
    "description": "string",
```

```
    "device_class": "string",
    "dhcp_name": "string",
    "discover_time": 0,
    "discovery_id": "string",
    "display_name": "string",
    "dns_name": "string",
    "extrahop_id": "string",
    "id": 0,
    "ipaddr4": "string",
    "ipaddr6": "string",
    "is_l3": true,
    "last_seen_time": 0,
    "macaddr": "string",
    "mod_time": 0,
    "model": "string",
    "model_override": "string",
    "netbios_name": "string",
    "node_id": 0,
    "on_watchlist": true,
    "parent_id": 0,
    "role": "string",
    "subnet_id": "string",
    "user_mod_time": 0,
    "vendor": "string",
    "vlanid": 0,
    "vpc_id": "string"
}
```

`PATCH /devices/{id}`

Specify the following parameters.

`body:` ***Object***

Apply the specified property value updates to the device.

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`GET /devices/{id}/activity`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "device_id": 0,
    "from_time": 0,
    "id": 0,
    "mod_time": 0,
    "stat_name": "string",
    "until_time": 0
}
```

`GET /devices/{id}/ipaddrs`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`from:` ***Number***

(Optional) Retrieves IP addresses that were associated with the device after the specified date, expressed in milliseconds since the epoch.

`until:` ***Number***

(Optional) Retrieves IP addresses that were associated with the device before the specified date, expressed in milliseconds since the epoch.

`GET /devices/{id}/dnsnames`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`from:` ***Number***

(Optional) Retrieves DNS names that were associated with the device after the specified date, expressed in milliseconds since the epoch.

`until:` ***Number***

(Optional) Retrieves DNS names that were associated with the device before the specified date, expressed in milliseconds since the epoch.

`GET /devices/{id}/triggers`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`direct_assignments_only:` ***Boolean***

(Optional) Restrict results to only triggers that are directly assigned to the device.

`POST /devices/{id}/triggers`

Specify the following parameters.

`body:` ***Object***

A list of unique identifiers for triggers that are assigned and unassigned to the device.

`assign:` ***Array of Numbers***

IDs of resources to assign

`unassign:` ***Array of Numbers***

IDs of resources to unassign

Specify the body parameter in the following JSON format.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`POST /devices/{id}/triggers/{child-id}`

Specify the following parameters.

`child-id:` ***Number***

The unique identifier for the trigger.

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`DELETE /devices/{id}/triggers/{child-id}`

Specify the following parameters.

`child-id:` ***Number***

The unique identifier for the trigger.

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`GET /devices/{id}/dashboards`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`GET /devices/{id}/devicegroups`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the device.

`active_from:` ***Number***

(Optional) The beginning timestamp for the request. Return only dynamic device groups that the device belonged to after this time. Time is expressed in milliseconds since the epoch. 0 indicates the time of the request. A negative value is evaluated relative to the current time. The default unit for a negative value is milliseconds, but other units can be specified with a unit suffix. See the REST API Guide for supported time units and suffixes.

`active_until:` ***Number***

(Optional) The ending timestamp for the request. Return only dynamic device groups that the device belonged to before this time. Follows the same time value guidelines as the active_from parameter.

`POST /devices/{id}/devicegroups`

Specify the following parameters.

`body:` ***Object***

The list of unique identifiers for device groups that are assigned and unassigned to the device.

`assign:` ***Array of Numbers***

IDs of resources to assign

`unassign:` ***Array of Numbers***

IDs of resources to unassign

Specify the body parameter in the following JSON format.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`POST /devices/{id}/devicegroups/{child-id}`

Specify the following parameters.

`child-id:` ***Number***

The unique identifier for the device group.

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`DELETE /devices/{id}/devicegroups/{child-id}`

Specify the following parameters.

`child-id:` ***Number***

The unique identifier for the device group.

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`GET /devices/{id}/tags`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`POST /devices/{id}/tags`

Specify the following parameters.

`body:` ***Object***

A list of unique identifiers for tags that are assigned and unassigned to the device.

`assign:` ***Array of Numbers***

IDs of resources to assign

`unassign:` ***Array of Numbers***

IDs of resources to unassign

Specify the body parameter in the following JSON format.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`POST /devices/{id}/tags/{child-id}`

Specify the following parameters.

`child-id:` ***Number***

The unique identifier for the tag.

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`DELETE /devices/{id}/tags/{child-id}`

Specify the following parameters.

`child-id:` ***Number***

The unique identifier for the tag.

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`GET /devices/{id}/alerts`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`direct_assignments_only:` ***Boolean***

(Optional) Restrict results to only alerts that are directly assigned to the device.

`POST /devices/{id}/alerts`

Specify the following parameters.

`body:` ***Object***

The list of unique identifiers for alerts that are assigned and unassigned to the device.

`assign:` ***Array of Numbers***

IDs of resources to assign

`unassign:` ***Array of Numbers***

IDs of resources to unassign

Specify the body parameter in the following JSON format.

```
{
    "assign": [],
```

```
    "unassign": []
}
```

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`POST /devices/{id}/alerts/{child-id}`

Specify the following parameters.

`child-id:` ***Number***

The unique identifier for the alert.

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`DELETE /devices/{id}/alerts/{child-id}`

Specify the following parameters.

`child-id:` ***Number***

The unique identifier for the alert.

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`GET /devices/{id}/software`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the device, which is displayed as the API ID on the device page in the ExtraHop system.

`from:` ***Number***

(Optional) Returns software that was observed on the device after the specified date, expressed in milliseconds since the epoch.

`until:` ***Number***

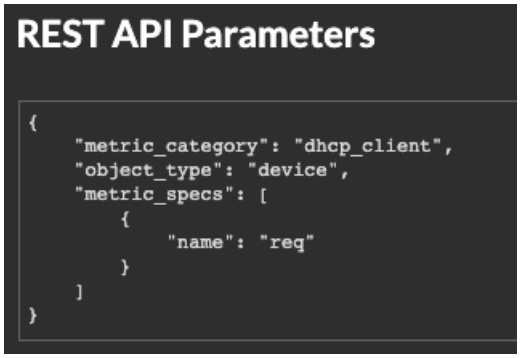
(Optional) Returns software that was observed on the device before the specified date, expressed in milliseconds since the epoch.

Operand values for device search

The POST /devices/search operation enables you to search for devices by criteria specified in filter objects. Each object should contain a unique value for the `operand` field that is valid for the specified `field` value.

`activity`

To search by metric activity, specify the `field` value as `activity` and the `operand` value as a `metric_category`. You can find `metric_category` values in the REST API Parameters section of the Metric Catalog.



The following example returns results for devices that match all metric activity classified for a DHCP client, such as the number of DHCP requests sent.

```
{
    "filter":  {
        "field": "activity",
        "operand": "dhcp_client",
        "operator": "="
    }
}
```

Tip: Programmatically retrieve a list of all metric activity for a device through the `GET /devices/{id}/activity` operation. The `stat_name` value matches the `metric_category` value in the `metric_catalog`, after the final dot.

In the following example response, the `stat_name` value is `extrahop.device.dhcp_client`. Remove the text before the final dot to identify the `metric_catalog` value of `dhcp_client`.

```
{
    "id": 198606,
    "from_time": 1581537120000,
    "until_time": 1581542520000,
    "mod_time": 1581542533963,
    "device_id": 30096,
    "stat_name": "extrahop.device.dhcp_client"
}
```

analysis

To search by device analysis level, specify the `field` value as `analysis` and the `operand` value as one of the following strings:

standard
Devices in Standard Analysis.

advanced
Devices in Advanced Analysis.

discovery
Devices in Discovery Mode.

l2_exempt
Devices in L2 Parent Analysis.

flow_log
Devices in Flow Analysis.

`discover_time`

To search by a time range, specify the `field` value as `discover_time` and an `operand` value with `from` and `until` parameters, where the values are dates, expressed in milliseconds since the epoch.

The following example returns results for all device activity that occurred between 1:00 PM to 3:00 PM on August 21, 2019.

```
{
    "filter":  {
        "field": "discover_time",
        "operand": {
            "from": "1566392400000",
            "until": "1566399600000"
        },
        "operator": "="
    }
}
```

`discovery_id`

To search by the unique ID for the device, specify the `field` value as `discovery_id` and the `operand` value as the discovery ID.

```
{
  "filter": {
    "field": "discovery_id",
    "operand": "c12vf90qpg290000",
    "operator": "="
  }
}
```

id

To retrieve multiple devices, specify the field value as `id`, the `operator` value as `in`, and the `operand` value as an array of IDs.

```
{
  "filter": {
    "field": "id",
    "operand": [5388,5387],
    "operator": "in"
  }
}
```

To exclude devices from search results, specify a filter with multiple rules, and specify a rule with the field value as `id`, the `operator` value as `not_in`, and the `operand` value as an array of IDs.

```
{
  "filter": {
    "operator": "and",
    "rules": [
      {
        "field": "id",
        "operand": [5388,5387],
        "operator": "not_in"
      },
      {
        "field": "discover_time",
        "operand": {
          "from": "1692984750000",
```

```
          "until": "1693416750000"
        },
        "operator": "="
      }
    ]
  }
}
```

is_active

To search by devices that have activity in the last 30 minutes, specify the field value as `is_active` and the `operand` value as a boolean.

```
{
  "filter": {
    "field": "is_active",
    "operand": true,
    "operator": "="
  }
}
```

`ipaddr`

To search by IP address, specify the `field` value as `ipaddr` and the `operand` value as an IP address or CIDR block.

```
{
  "filter": {
    "field": "ipaddr",
    "operand": "192.168.12.0/28",
    "operator": "="
  }
}
```

`node`

To search by the unique ID of a sensor, specify the `field` value as `node` and the `operand` value as the sensor UUID.

```
{
  "filter": {
    "field": "node",
    "operand": "qqvsplfa-zxsk-32l0-19g1-076vfr42pw31",
    "operator": "="
  }
}
```

`macaddr`

To search by the MAC address of a device, specify the field value as `macaddr` and the operand value as the device MAC address. The following example returns results for devices with a MAC address of `C1:1C:N2:0Q:PJ:10` or `C1:1C:N2:0Q:PJ:11`.

```
{
  "filter": {
    "operator": "or",
    "rules": [
      {
        "field": "macaddr",
```

```
        "operand": "C1:1C:N2:0Q:PJ:10",
        "operator": "="
      },
      {
        "field": "macaddr",
        "operand": "C1:1C:N2:0Q:PJ:11",
        "operator": "="
      }
    ]
  }
}
```

`name`

To search by the device display name, specify the `field` value as name and the `operand` value as the device name or as a regex string.

```
{
  "filter": {
    "field": "name",
    "operand": "VMware B2CEB6",
    "operator": "="
  }
}
```

network_locality_id

To search by network locality, specify the `field` value as `network_locality_id` and the operand value as a network locality ID.

```
{
  "filter": {
    "field": "network_locality_id",
    "operand": 123,
    "operator": "="
  }
}
```

`role`

To search by the device role, specify the `field` value as `role` and the `operand` value as the device role.

```
{
  "filter": {
    "field": "role",
    "operand": "voip_phone",
    "operator": "="
  }
}
```

`software`

To search by the software running on the device, specify the `field` value as `software` and the `operand` value as the ID associated with that software on the ExtraHop system or as a regex string.

```
{
  "filter": {
    "field": "software",
    "operand": "windows_10",
```

```
    "operator": "="
  }
}
```

Tip: Programmatically retrieve a list of all software IDs associated with a device through the `GET /devices/{id}/software` operation.

In the following example response, the `id` value for the software is `windows_10`.

```
[
  {
    "software_type": "OS",
    "name": "Windows",
    "version": "10",
    "description": null,
    "id": "windows_10"
  }
]
```

`tag`

To search by a device tag, specify the `field` value as `tag` and the `operand` value as the tag name or as a regex string.

```
{
  "filter": {
    "field": "tag",
    "operand": "Custom Tag",
    "operator": "="
  }
}
```

Tip: Programmatically retrieve a list of all device tags through the `GET /devices/{id}/tags` operation.

In the following example response, the `name` value for the tag is `Custom Tag`.

```
[
  {
    "mod_time": 1521577040934,
    "id": 19,
    "name": "Custom Tag"
  }
]
```

vlan

To search by the ID of a VLAN, specify the `field` value as `vlan` and the `operand` value as the ID of the VLAN.

```
{
  "filter": {
    "field": "vlan",
    "operand": "0",
    "operator": "="
  }
}
```

Search with regular expressions (regex)

For certain `field` values, the string can be in regex syntax. Specify the `operand` value as an object that has a `value` parameter with the regex syntax you want to match and an `is_regex` parameter that is set to `true`. The following example returns results for all DNS names that end with `com`.

```
{
    "filter":  {
        "field": "dns_name",
        "operand": {
            "value": ".*?com",
            "is_regex": true
        },
        "operator": "="
    }
}
```

An `operand` field with regex syntax is valid for the following `field` values:

- cdp_name
- custom_name
- dns_name
- dhcp_name
- model
- name
- netbios_name
- software
- tag
- vendor

Supported time units

For most parameters, the default unit for time measurement is milliseconds. However, the following parameters return or accept alternative time units such as minutes and hours:

- Device
  - active_from
  - active_until
- Device group
  - active_from
  - active_until
- Metrics
  - from
  - until
- Record Log
  - from
  - until
  - context_ttl

The following table displays supported time units:

Time unit	Unit suffix
Year	y
Month	M

Time unit	Unit suffix
Week	w
Day	d
Hour	h
Minute	m
Second	s
Millisecond	ms

To specify a time unit other than milliseconds for a parameter, append the unit suffix to the value. For example, to request devices active in the last 30 minutes, specify the following parameter value:

```
GET /api/v1/devices?active_from=-30m
```

The following example specifies a search for HTTP records created between 1 and 2 hours ago:

```
{
    "from": "-2h",
    "until": "-1h",
    "types": ["~http"]
}
```

Exclusion intervals

An exclusion interval can be created to set a time period to suppress an alert.

For example, if you do not want to be notified about alerts after hours or on the weekends, an exclusion interval can create a rule to suppress the alert during that time period. For more information, see Alerts.

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /exclusionintervals	Retrieve all exclusion intervals.
POST /exclusionintervals	Create a new exclusion interval.
DELETE /exclusionintervals/{id}	Delete a specific exclusion interval.
GET /exclusionintervals/{id}	Retrieve a specific exclusion interval.
PATCH /exclusionintervals/{id}	Apply updates to a specific exclusion interval.

Operation details

`GET /exclusionintervals`

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "alert_apply_all": true,
    "author": "string",
    "description": "string",
    "end": 0,
    "id": 0,
```

```
    "interval_type": "string",
    "mod_time": 0,
    "name": "string",
    "start": 0,
    "trend_apply_all": true
}
```

`POST /exclusionintervals`

Specify the following parameters.

`body:` ***Object***

Set the specified property values on the new exclusion interval.

`name:` ***String***

The friendly name for the exclusion interval.

`author:` ***String***

(Optional) The name of the creator of the exclusion interval.

`description:` ***String***

(Optional) An optional description of the exclusion interval.

`interval_type:` ***String***

The time window when the exclusion interval was evaluated.

The following values are valid:

- `onetime`
- `weekly`
- `daily`

`start:` ***Number***

The start of the exclusion interval time range, expressed in seconds. This value is relative to the epoch for onetime exclusions, relative to midnight for daily exclusions, and relative to Monday at midnight for weekly exclusions.

`end:` ***Number***

The end of the exclusion interval time range, expressed in seconds. This value is relative to the epoch for onetime exclusions, relative to midnight for daily exclusions, and relative to Monday at midnight for weekly exclusions.

`alert_apply_all:` ***Boolean***

Indicates whether this exclusion interval should be applied to all alerts.

`trend_apply_all:` ***Boolean***

Indicates whether this exclusion interval should be applied to all trends.

Specify the body parameter in the following JSON format.

```
{
    "alert_apply_all": true,
    "author": "string",
    "description": "string",
    "end": 0,
    "interval_type": "string",
    "name": "string",
    "start": 0,
    "trend_apply_all": true
}
```

`GET /exclusionintervals/{id}`

Specify the following parameters.

`id:` ***Number***
The unique identifier of the exclusion interval.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "alert_apply_all": true,
    "author": "string",
    "description": "string",
    "end": 0,
    "id": 0,
    "interval_type": "string",
    "mod_time": 0,
    "name": "string",
    "start": 0,
    "trend_apply_all": true
}
```

`DELETE /exclusionintervals/{id}`

Specify the following parameters.

`id:` ***Number***
The unique identifier of the exclusion interval.

`PATCH /exclusionintervals/{id}`

Specify the following parameters.

`body:` ***Object***
Apply the specified property value updates to the exclusion interval.

`id:` ***Number***
The unique identifier for the exclusion interval.

Metrics

Metrics information is collected about every object identified by the ExtraHop system.

Note that metrics are retrieved through the POST method, which creates a query to collect the requested information through the API. For more information, see Extract metrics through the REST API.

The following table displays all of the operations you can perform on this resource:

Operation	Description
POST /metrics	Perform a metric query.
GET /metrics/next/{xid}	If a previous metric query requested activity group metrics from a console, the GET /metrics/next/{xid} operation retrieves metrics for the activity group on a connected sensor. Each time a request is sent to GET /metrics/next/{xid}, the operation returns metrics from a different sensor. After all metrics have been retrieved, the operation returns null.

Operation	Description
POST /metrics/total	Perform a metric query for total values.
POST /metrics/totalbyobject	Perform a metric query for total values that are grouped by object.

For example, if you want to see all HTTP responses that occurred on the network in the last 30 minutes, enter the following request schema into the `POST /metrics` operation:

```
{
  "cycle": "auto",
  "from": -1800000,
  "metric_category": "http",
  "metric_specs": [
    {
      "name": "rsp"
    }
  ],
  "object_ids": [
    0
  ],
  "object_type": "application",
  "until": 0
}
```

The response body returns a list of HTTP responses and the time of each event, similar to the following output:

```
{
  "stats": [
    {
      "oid": 0,
      "time": 1494539640000,
      "duration": 30000,
      "values": [
        354
      ]
    },
    {
      "oid": 0,
      "time": 1494539640000,
      "duration": 30000,
      "values": [
        354
      ]
    },

    {
      "oid": 0,
      "time": 1494539640000,
      "duration": 30000,
      "values": [
        354
      ]
    },
  ],
  "cycle": "30sec",
  "node_id": 0,
  "clock": 1494541440000,
  "from": 1494539640000,
  "until": 1494541440000
```

```
}
```

Enter the same request schema into the `POST /metrics/total` operation to retrieve a count of all HTTP responses that occurred on the network in the last 30 seconds. The response body is similar to the following output:

```
{
  "stats": [
    {
      "oid": -1,
      "time": 1494541380000,
      "duration": 1800000,
      "values": [
        33357
      ]
    }
  ],
  "cycle": "30sec",
  "node_id": 0,
  "clock": 1494541440000,
  "from": 1494539640000,
  "until": 1494541440000
}
```

Operation details

`POST /metrics`

Specify the following parameters.

`body:` ***Object***

The description of the metric request.

`from:` ***Number***

The beginning timestamp for the request. Return only metrics collected after this time. Time is expressed in milliseconds since the epoch. 0 indicates the time of the request. A negative value is evaluated relative to the current time. The default unit for a negative value is milliseconds, but other units can be specified with a unit suffix. See the REST API Guide for supported time units and suffixes.

`until:` ***Number***

The ending timestamp for the request. Return only metrics collected before this time. Follows the same time value guidelines as the from parameter.

`cycle:` ***String***

The aggregation period for metrics.

The following values are valid:

- `auto`
- `1sec`
- `30sec`
- `5min`
- `1hr`
- `24hr`

`object_type:` ***String***

Indicates the object type of unique identifiers specified in the object_ids property.

The following values are valid:

- `network`
- `device`
- `application`
- `vlan`
- `device_group`
- `system`

`object_ids:` ***Array of Numbers***

The list of numeric values that represent unique identifiers. Unique identifiers can be retrieved through the /networks, /devices, /applications, /vlans, /devicegroups, /activitygroups, and /appliances resources. For system health metrics, specify the ID of the sensor or console and set the object_type parameter to "system".

`metric_category:` ***String***

The group of metrics that are searchable in the metric catalog.

`metric_specs:` ***Array of Objects***

An array of metric specification objects.

`name:` ***String***

The field name for the metric. When filtering in the metric catalog on a metric_category, each result is a potential metric_spec name. When a result is selected from the catalog, the "Metric" field value is a valid option for this field.

`key1:` ***String***

(Optional) Filter detail metrics. Detail metrics break down data through keys, which are strings or IP addresses. For example, the metric "HTTP Requests by Method" accepts a key1 value of "GET." Keys can also be regular expressions that are delimited with forward slashes ("/GET/").

`key2:` ***String***

(Optional) Enable additional filtering on detail metrics.

`calc_type:` ***String***

(Optional) The type of calculation to perform.

The following values are valid:

- `mean`
- `percentiles`

`percentiles:` ***Array of Numbers***

(Optional) The list of percentiles, sorted in ascending order, which should be returned. This parameter is only required if the calc_type parameter is set to "percentiles". If the calc_type parameter is set to mean, the percentiles property cannot be set.

Specify the body parameter in the following JSON format.

```
{
    "cycle": "string",
    "from": 0,
    "metric_category": "string",
    "metric_specs": {
        "name": "string",
        "key1": "string",
        "key2": "string",
        "calc_type": "string",
        "percentiles": []
    },
    "object_ids": [],
    "object_type": "string",
    "until": 0
```

```
}
```

`POST /metrics/total`

Specify the following parameters.

`body:` ***Object***

The description of the metric request.

`from:` ***Number***

The beginning timestamp for the request. Return only metrics collected after this time. Time is expressed in milliseconds since the epoch. 0 indicates the time of the request. A negative value is evaluated relative to the current time. The default unit for a negative value is milliseconds, but other units can be specified with a unit suffix. See the REST API Guide for supported time units and suffixes.

`until:` ***Number***

The ending timestamp for the request. Return only metrics collected before this time. Follows the same time value guidelines as the from parameter.

`cycle:` ***String***

The aggregation period for metrics.

The following values are valid:

- `auto`
- `1sec`
- `30sec`
- `5min`
- `1hr`
- `24hr`

`object_type:` ***String***

Indicates the object type of unique identifiers specified in the object_ids property.

The following values are valid:

- `network`
- `device`
- `application`
- `vlan`
- `device_group`
- `system`

`object_ids:` ***Array of Numbers***

The list of numeric values that represent unique identifiers. Unique identifiers can be retrieved through the /networks, /devices, /applications, /vlans, /devicegroups, /activitygroups, and /appliances resources. For system health metrics, specify the ID of the sensor or console and set the object_type parameter to "system".

`metric_category:` ***String***

The group of metrics that are searchable in the metric catalog.

`metric_specs:` ***Array of Objects***

An array of metric specification objects.

`name:` ***String***

The field name for the metric. When filtering in the metric catalog on a metric_category, each result is a potential metric_spec name. When a result is selected from the catalog, the "Metric" field value is a valid option for this field.

`key1:` ***String***

(Optional) Filter detail metrics. Detail metrics break down data through keys, which are strings or IP addresses. For example, the metric "HTTP Requests by Method" accepts a key1 value of "GET." Keys can also be regular expressions that are delimited with forward slashes ("/GET/").

`key2:` ***String***

(Optional) Enable additional filtering on detail metrics.

`calc_type:` ***String***

(Optional) The type of calculation to perform.

The following values are valid:

- `mean`
- `percentiles`

`percentiles:` ***Array of Numbers***

(Optional) The list of percentiles, sorted in ascending order, which should be returned. This parameter is only required if the calc_type parameter is set to "percentiles". If the calc_type parameter is set to mean, the percentiles property cannot be set.

Specify the body parameter in the following JSON format.

```
{
    "cycle": "string",
    "from": 0,
    "metric_category": "string",
    "metric_specs": {
        "name": "string",
        "key1": "string",
        "key2": "string",
        "calc_type": "string",
        "percentiles": []
    },
    "object_ids": [],
    "object_type": "string",
    "until": 0
}
```

`POST /metrics/totalbyobject`

Specify the following parameters.

`body:` ***Object***

The description of the metric request.

`from:` ***Number***

The beginning timestamp for the request. Return only metrics collected after this time. Time is expressed in milliseconds since the epoch. 0 indicates the time of the request. A negative value is evaluated relative to the current time. The default unit for a negative value is milliseconds, but other units can be specified with a unit suffix. See the REST API Guide for supported time units and suffixes.

`until:` ***Number***

The ending timestamp for the request. Return only metrics collected before this time. Follows the same time value guidelines as the from parameter.

`cycle:` ***String***

The aggregation period for metrics.

The following values are valid:

- `auto`
- `1sec`
- `30sec`
- `5min`
- `1hr`
- `24hr`

`object_type:` ***String***

Indicates the object type of unique identifiers specified in the object_ids property.

The following values are valid:

- `network`
- `device`
- `application`
- `vlan`
- `device_group`
- `system`

`object_ids:` ***Array of Numbers***

The list of numeric values that represent unique identifiers. Unique identifiers can be retrieved through the /networks, /devices, /applications, /vlans, /devicegroups, /activitygroups, and /appliances resources. For system health metrics, specify the ID of the sensor or console and set the object_type parameter to "system".

`metric_category:` ***String***

The group of metrics that are searchable in the metric catalog.

`metric_specs:` ***Array of Objects***

An array of metric specification objects.

`name:` ***String***

The field name for the metric. When filtering in the metric catalog on a metric_category, each result is a potential metric_spec name. When a result is selected from the catalog, the "Metric" field value is a valid option for this field.

`key1:` ***String***

(Optional) Filter detail metrics. Detail metrics break down data through keys, which are strings or IP addresses. For example, the metric "HTTP Requests by Method" accepts a key1 value of "GET." Keys can also be regular expressions that are delimited with forward slashes ("/GET/").

`key2:` ***String***

(Optional) Enable additional filtering on detail metrics.

`calc_type:` ***String***

(Optional) The type of calculation to perform.

The following values are valid:

- `mean`
- `percentiles`

`percentiles:` ***Array of Numbers***

(Optional) The list of percentiles, sorted in ascending order, which should be returned. This parameter is only required if the calc_type parameter is set to "percentiles". If the calc_type parameter is set to mean, the percentiles property cannot be set.

Specify the body parameter in the following JSON format.

```
{
    "cycle": "string",
```

```
    "from": 0,
    "metric_category": "string",
    "metric_specs": {
        "name": "string",
        "key1": "string",
        "key2": "string",
        "calc_type": "string",
        "percentiles": []
    },
    "object_ids": [],
    "object_type": "string",
    "until": 0
}
```

`GET /metrics/next/{xid}`

Specify the following parameters.

`xid:` ***Number***

The unique identifier returned by a metric query.

Supported time units

For most parameters, the default unit for time measurement is milliseconds. However, the following parameters return or accept alternative time units such as minutes and hours:

- Device
  - active_from
  - active_until
- Device group
  - active_from
  - active_until
- Metrics
  - from
  - until
- Record Log
  - from
  - until
  - context_ttl

The following table displays supported time units:

Time unit	Unit suffix
Year	y
Month	M
Week	w
Day	d
Hour	h
Minute	m
Second	s

Time unit	Unit suffix
Millisecond	ms

To specify a time unit other than milliseconds for a parameter, append the unit suffix to the value. For example, to request devices active in the last 30 minutes, specify the following parameter value:

```
GET /api/v1/devices?active_from=-30m
```

The following example specifies a search for HTTP records created between 1 and 2 hours ago:

```
{
    "from": "-2h",
    "until": "-1h",
    "types": ["~http"]
}
```

Network locality entry

You can manage a list that specifies the network locality of IP addresses.

For example, you can create an entry in the network locality list that specifies that an IP address or CIDR block is internal or external.

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /networklocalities	Retrieve all network locality entries.
POST /networklocalities	Create a network locality entry.
DELETE /networklocalities/{id}	Delete a network locality entry.
GET /networklocalities/{id}	Retrieve a specific network locality entry.
PATCH /networklocalities/{id}	Apply updates to a specific network locality entry.

Operation details

`GET /networklocalities`

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "description": "string",
    "external": true,
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "network": "string",
    "networks": []
}
```

`POST /networklocalities`

Specify the following parameters.

`body:` ***Object***

Apply the specified property values to the new network locality entry.

`name:` ***String***

(Optional) The name of the network locality. If this field is not specified, the network locality is named in the following format: "locality_ID", where ID is the unique identifier of the network locality.

`network:` ***String***

(Optional) Deprecated. Specify CIDR blocks or IP addresses with the networks field.

`networks:` ***Array of Strings***

(Optional) An array of CIDR blocks or IP addresses that define the network locality.

`external:` ***Boolean***

Indicates whether the network is internal or external.

`description:` ***String***

(Optional) An optional description of the network locality entry.

Specify the body parameter in the following JSON format.

```
{
    "description": "string",
    "external": true,
    "name": "string",
    "network": "string",
    "networks": []
}
```

`GET /networklocalities/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the network locality entry.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "description": "string",
    "external": true,
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "network": "string",
    "networks": []
}
```

`DELETE /networklocalities/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the network locality entry.

`PATCH /networklocalities/{id}`

Specify the following parameters.

`body:` ***Object***

Apply the specified property value updates to the network locality entry.

`network:` ***String***

(Optional) Deprecated. Specify CIDR blocks or IP addresses with the networks field.

`networks:` ***Array of Strings***

(Optional) An array of CIDR blocks or IP addresses that define the network locality.

`name:` ***String***

(Optional) The name of the network locality.

`external:` ***Boolean***

(Optional) Indicates whether the network is internal or external.

`description:` ***String***

(Optional) An optional description of the network locality entry.

Specify the body parameter in the following JSON format.

```
{
    "description": "string",
    "external": true,
    "name": "string",
    "network": "string",
    "networks": []
}
```

`id:` ***Number***

The unique identifier for the network locality entry.

Network

Networks are correlated to the network interface card that receives input from all of the objects identified by the ExtraHop system.

On a console, each connected sensor is identified as a network capture. For more information, see Networks.

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /networks	Retrieve all networks.
GET /networks/{id}	Retreive a specific network by ID.
PATCH /networks/{id}	Update a specific network by ID.
GET /networks/{id}/alerts	Retrieve all alerts that are assigned to a specific network.
POST /networks/{id}/alerts	Assign and unassign alerts to a specific network.
DELETE /networks/{id}/alerts/{child-id}	Unassign an alert from a specific network.
POST /networks/{id}/alerts/{child-id}	Assign an alert to a specific network.
GET /networks/{id}/vlans	Retrieve all VLANS assigned to a specific network.

Operation details

`GET /networks`

There are no parameters for this operation.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "appliance_uuid": "string",
    "description": "string",
    "id": 0,
    "idle": true,
    "mod_time": 0,
    "name": "string",
    "node_id": 0
}
```

`PATCH /networks/{id}`

Specify the following parameters.

`body:` ***Object***
Property value updates to apply to the network.

`id:` ***Number***
Unique identifier of the network.

`GET /networks/{id}`

Specify the following parameters.

`id:` ***Number***
Unique identifier of the network.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "appliance_uuid": "string",
    "description": "string",
    "id": 0,
    "idle": true,
    "mod_time": 0,
    "name": "string",
    "node_id": 0
}
```

`GET /networks/{id}/alerts`

Specify the following parameters.

`id:` ***Number***
Unique identifier of the network.

`direct_assignments_only:` ***Boolean***
(Optional) Restrict results to only alerts directly assigned to the network.

`POST /networks/{id}/alerts`

Specify the following parameters.

`body:` ***Object***

Lists of alert IDs to assign and/or unassign.

`assign:` ***Array of Numbers***

IDs of resources to assign

`unassign:` ***Array of Numbers***

IDs of resources to unassign

Specify the body parameter in the following JSON format.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Number***

Unique identifier of the network.

`POST /networks/{id}/alerts/{child-id}`

Specify the following parameters.

`child-id:` ***Number***

Unique identifier of the alert.

`id:` ***Number***

Unique identifier of the network.

`DELETE /networks/{id}/alerts/{child-id}`

Specify the following parameters.

`child-id:` ***Number***

Unique identifier of the alert.

`id:` ***Number***

Unique identifier of the network.

`GET /networks/{id}/vlans`

Specify the following parameters.

`id:` ***Number***

Unique identifier of the network.

Observations

An observation associates the IP address of a device on the ExtraHop system with an IP address outside of your network. For example, you can track the activity of a VPN user by associating the IP address of the VPN client on your internal network with the external IP address assigned to the user on the public internet.

The following table displays all of the operations you can perform on this resource:

Operation	Description
POST /observations/associatedipaddrs	Add an observation to create an association between device IP addresses.

Operation details

`POST /observations/associatedipaddrs`

Specify the following parameters.

`body:` ***Object***

The observation parameters.

`observations:` ***Array of Objects***

An array of observations.

`ipaddr:` ***String***

The device IP address observed by the sensor or console.

`associated_ipaddr:` ***String***

The associated IP address.

`timestamp:` ***Number***

The time that the observation was created by the source, expressed in milliseconds since the epoch.

`source:` ***String***

The source of the observations.

Specify the body parameter in the following JSON format.

```
{
    "observations": {
        "ipaddr": "string",
        "associated_ipaddr": "string",
        "timestamp": 0
    },
    "source": "string"
}
```

Packet Search

You can search for and download packets stored on the ExtraHop system. The downloaded packets can then be analyzed through a third-party tool, such as Wireshark.

For more information about Packets, see Packets.

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /packets/search	Search for packets by specifying parameters in a URL.
POST /packets/search	Search for packets by specifying parameters in a JSON string.

Operation details

```
GET /packets/search
```

Specify the following parameters.

`output:` ***String***

(Optional) The output format. * `pcap` - A PCAP file that contains packets. * `keylog_txt` - A keylog text file that contains secrets for decryption. * `pcapng` - A PCAPNG file that can contain both packets and secrets for decryption. * `zip` - A ZIP file that contains both a PCAP and keylog text file.

The following values are valid:

- `pcap`
- `keylog_txt`
- `pcapng`
- `zip`

`include_secrets:` ***Boolean***

(Optional) Specifies whether to include secrets in the PCAPNG file. This option is valid only if `output` is set to `pcapng`.

`limit_bytes:` ***String***

(Optional) The approximate maximum number of bytes to return. After the ExtraHop system finds packets that match the size specified in the search criteria, the system stops searching for additional packets. However, because the system analyzes multiple packets at a time, the total size of the packets returned might be larger than the specified size. The default unit is bytes, but you can specify other units with a unit suffix. The default value is "100MB".

`limit_search_duration:` ***String***

(Optional) The approximate maximum amount of time to perform the packet search. After the specified amount of time has passed, the ExtraHop system stops searching for additional packets. However, the system will extend past the specified time to finish analyzing packets that were being searched before the time expired, and the system analyzes multiple packets at a time. Therefore, the search might last longer than the specified time. The default unit is milliseconds, but other units can be specified with a unit suffix. See the REST API Guide for supported time units and suffixes. The default value is "5m".

`always_return_body:` ***Boolean***

(Optional) If you set this parameter to true, and the search does not match any packets, the system returns an empty packet capture file and an HTTP status of 200. If you set this parameter to false, and the search does not match any packets, the system returns no packet capture file and an HTTP status of 204.

`from:` ***String***

The beginning timestamp of the time range the search will include, expressed in milliseconds since the epoch. A negative value specifies that the search will begin with packets captured at a time in the past. For example, specify -10m to begin the search with packets captured 10 minutes before the time of the request. Negative values can be specified with a time unit other than milliseconds, such as seconds or hours. See the REST API Guide for supported time units and suffixes.

`until:` ***String***

(Optional) The ending timestamp of the time range the search will include, expressed in milliseconds since the epoch. A 0 value specifies that the search will end with packets captured at the time of the search. A negative value specifies that the search will end with packets captured at a time in the past. For example, specify -5m to end the search with packets captured 5 minutes before the time of the request. Negative values can be specified with a time unit other than milliseconds, such as seconds or hours. See the REST API Guide for supported time units and suffixes.

`bpf:` ***String***

(Optional) The Berkeley Packet Filter (BPF) syntax for the packet search. For more information about BPF syntax, see the REST API Guide.

`ip1:` ***String***

(Optional) Returns packets sent to or received by the specified IP address.

`port1:` ***String***

(Optional) Returns packets sent from or received on the specified port.

`ip2:` ***String***

(Optional) Returns packets sent to or received by the specified IP address.

`port2:` ***String***

(Optional) Returns packets sent from or received on the specified port.

`POST /packets/search`

Specify the following parameters.

`body:` ***Object***

The parameters of the packet search.

`output:` ***String***

(Optional) The output format.

The following values are valid:

- `pcap`
- `keylog_txt`
- `pcapng`
- `zip`

`include_secrets:` ***Boolean***

(Optional) Whether or not to include TLS secrets together with packet data in .pcapng files. Only valid if "output" is "pcapng".

`limit_bytes:` ***String***

(Optional) The approximate maximum number of bytes to return. After the ExtraHop system finds packets that match the size specified in the search criteria, the system stops searching for additional packets. However, because the system analyzes multiple packets at a time, the total size of the packets returned might be larger than the specified size. The default unit is bytes, but you can specify other units with a unit suffix. The default value is "100MB".

`limit_search_duration:` ***String***

(Optional) The approximate maximum amount of time to perform the packet search. After the specified amount of time has passed, the ExtraHop system stops searching for additional packets. However, the system will extend past the specified time to finish analyzing packets that were being searched before the time expired, and the system analyzes multiple packets at a time. Therefore, the search might last longer than the specified time. The default unit is milliseconds, but other units can be specified with a unit suffix. See the REST API Guide for supported time units and suffixes. The default value is "5m".

`always_return_body:` ***Boolean***

(Optional) If you set this parameter to true, and the search does not match any packets, the system returns an empty packet capture file and an HTTP status of 200. If you set this parameter to false, and the search does not match any packets, the system returns no packet capture file and an HTTP status of 204.

`from:` ***String***

The beginning timestamp of the time range the search will include, expressed in milliseconds since the epoch. A negative value specifies that the search will begin with packets captured at a time in the past. For example, specify -10m to begin the search with packets captured 10 minutes before the time of the request. Negative values can be specified with a time unit other than milliseconds, such as seconds or hours. See the REST API Guide for supported time units and suffixes.

`until:` ***String***

(Optional) The ending timestamp of the time range the search will include, expressed in milliseconds since the epoch. A 0 value specifies that the search will end with packets captured at the time of the search. A negative value specifies that the search will end with packets captured at a time in the past. For example, specify -5m to end the search with packets captured 5 minutes before the time of the request. Negative values can be specified with a time unit other than milliseconds, such as seconds or hours. See the REST API Guide for supported time units and suffixes.

`bpf:` ***String***

(Optional) The Berkeley Packet Filter (BPF) syntax for the packet search. For more information about BPF syntax, see Filter packets with Berkeley Packet Filter syntax.

`ip1:` ***String***

(Optional) Returns packets sent to or received by the specified IP address.

`port1:` ***String***

(Optional) Returns packets sent from or received on the specified port.

`ip2:` ***String***

(Optional) Returns packets sent to or received by the specified IP address.

`port2:` ***String***

(Optional) Returns packets sent from or received on the specified port.

Specify the body parameter in the following JSON format.

```
{
    "always_return_body": true,
    "bpf": "string",
    "from": "string",
    "include_secrets": true,
    "ip1": "string",
    "ip2": "string",
    "limit_bytes": "string",
    "limit_search_duration": "string",
    "output": "string",
    "port1": "string",
    "port2": "string",
    "until": "string"
}
```

Pairing

This resource enables you to generate a token required to connect a sensor to a console.

The following table displays all of the operations you can perform on this resource:

Operation	Description
POST /pairing/token	Generate a token required to connect the sensor to a console.

Operation details

```
POST /pairing/token
```

There are no parameters for this operation.

Report

A report is a PDF file of a dashboard that you can schedule for email delivery to one or more recipients. You can specify how often the report email is delivered and the time interval for dashboard data included in the PDF file.

Important: You can only schedule reports from an ECA VM.

Here are some important considerations about dashboard reports:

- You can only create a report for dashboards that you own or have been shared with you. Your ability to create a report is determined by your user privileges. Contact your ExtraHop administrator for help.
- Each report can only link to one dashboard.
- If you created a report for a dashboard that was later deleted or became inaccessible to you, the scheduled email will continue to be sent to recipients. However, the email will not include the PDF file and will instead notify recipients that the dashboard is unavailable to the report owner.

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /reports	Retrieve all reports.
POST /reports	Create a report.
DELETE /reports/{id}	Delete a specific report.
GET /reports/{id}	Retrieve a specific report.
PATCH /reports/{id}	Update a specific report.
GET /reports/{id}/contents	Retrieve the contents of a specific report.
PUT /reports/{id}/contents	Replace the contents of a specific report.
GET /reports/{id}/download	Retrieve the PDF of a report.
POST /reports/{id}/queue	Immediately generate and send a specific report.

Operation details

```
GET /reports
```

There are no parameters for this operation.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "cc": [],
    "description": "string",
```

```
    "email_message": "string",
    "email_subject": "string",
    "enabled": true,
    "from": "string",
    "id": 0,
    "include_links": "string",
    "name": "string",
    "output": {},
    "owner": "string",
    "schedule": {},
    "until": "string"
}
```

`POST /reports`

Specify the following parameters.

`body:` ***Object***

The contents of the report.

`name:` ***String***

The name of the report.

`description:` ***String***

(Optional) The description of the report.

`owner:` ***String***

The username of the report owner.

`cc:` ***Array of Strings***

The list of email addresses, not included in an email group, to receive reports.

`enabled:` ***Boolean***

(Optional) Indicates whether the report is enabled.

`from:` ***String***

The beginning timestamp of the time interval for the report contents, relative to the current time and expressed in milliseconds.

`until:` ***String***

(Optional) The ending timestamp of the time interval for the report contents, relative to the current time and expressed in milliseconds.

`email_subject:` ***String***

(Optional) The content of the subject line for the report email.

`schedule:` ***Object***

(Optional) The object containing the parameters that specify the scheduled time range to generate and send the report. The parameters are defined in the schedule_type section below.

`type:` ***String***

The type of delivery schedule for the report.

The following values are valid:

- `hourly`
- `daily`
- `weekly`

`at:` ***Array of Objects***

(Optional) The list of objects that specify the delivery parameters for the report. The parameters are defined in the at_type section below.

`by_day:` ***Array of Strings***

(Optional) The days of the week to send the report.

The following values are valid:

- `mo`
- `tu`
- `we`
- `th`
- `fr`
- `sa`
- `su`

`tz:` ***String***

(Optional) The timezone in which to send the report.

`hour:` ***Number***

(Optional) The hour at which to send the report.

`minute:` ***Number***

(Optional) The minute at which to send the report.

`output:` ***Object***

The object containing the parameters that specify the output format for the report. The parameters are defined in the format_type section below.

`type:` ***String***

The output format for the report.

The following values are valid:

- `pdf`

`width:` ***String***

(Optional) The width option for the report output.

The following values are valid:

- `narrow`
- `medium`
- `wide`

`pagination:` ***String***

(Optional) The pagination scheme for the report output.

The following values are valid:

- `per_region`

`theme:` ***String***

(Optional) The display theme for the report output.

The following values are valid:

- `light`
- `dark`
- `space`
- `contrast`

Specify the body parameter in the following JSON format.

```
{
    "cc": [],
    "description": "string",
```

```
    "email_subject": "string",
    "enabled": true,
    "from": "string",
    "name": "string",
    "output": {
        "type": "string",
        "width": "string",
        "pagination": "string",
        "theme": "string"
    },
    "owner": "string",
    "schedule": {
        "type": "string",
        "at": {
            "by_day": [],
            "tz": "string",
            "hour": 0,
            "minute": 0
        }
    },
    "until": "string"
}
```

`POST /reports/{id}/queue`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the report.

`PATCH /reports/{id}`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the report.

`body:` ***Object***
The contents of the report.

`name:` ***String***
The name of the report.

`description:` ***String***
(Optional) The description of the report.

`owner:` ***String***
The username of the report owner.

`cc:` ***Array of Strings***
The list of email addresses, not included in an email group, to receive reports.

`enabled:` ***Boolean***
(Optional) Indicates whether the report is enabled.

`from:` ***String***
The beginning timestamp of the time interval for the report contents, relative to the current time and expressed in milliseconds.

`until:` ***String***
(Optional) The ending timestamp of the time interval for the report contents, relative to the current time and expressed in milliseconds.

`email_subject:` ***String***

(Optional) The content of the subject line for the report email.

`schedule:` ***Object***

(Optional) The object containing the parameters that specify the scheduled time range to generate and send the report. The parameters are defined in the schedule_type section below.

`type:` ***String***

The type of delivery schedule for the report.

The following values are valid:

- `hourly`
- `daily`
- `weekly`

`at:` ***Array of Objects***

(Optional) The list of objects that specify the delivery parameters for the report. The parameters are defined in the at_type section below.

`by_day:` ***Array of Strings***

(Optional) The days of the week to send the report.

The following values are valid:

- `mo`
- `tu`
- `we`
- `th`
- `fr`
- `sa`
- `su`

`tz:` ***String***

(Optional) The timezone in which to send the report.

`hour:` ***Number***

(Optional) The hour at which to send the report.

`minute:` ***Number***

(Optional) The minute at which to send the report.

`output:` ***Object***

The object containing the parameters that specify the output format for the report. The parameters are defined in the format_type section below.

`type:` ***String***

The output format for the report.

The following values are valid:

- `pdf`

`width:` ***String***

(Optional) The width option for the report output.

The following values are valid:

- `narrow`
- `medium`
- `wide`

`pagination:` ***String***

(Optional) The pagination scheme for the report output.

The following values are valid:

- `per_region`

`theme:` ***String***

(Optional) The display theme for the report output.

The following values are valid:

- `light`
- `dark`
- `space`
- `contrast`

Specify the body parameter in the following JSON format.

```
{
    "cc": [],
    "description": "string",
    "email_subject": "string",
    "enabled": true,
    "from": "string",
    "name": "string",
    "output": {
        "type": "string",
        "width": "string",
        "pagination": "string",
        "theme": "string"
    },
    "owner": "string",
    "schedule": {
        "type": "string",
        "at": {
            "by_day": [],
            "tz": "string",
            "hour": 0,
            "minute": 0
        }
    },
    "until": "string"
}
```

`GET /reports/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the report.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "cc": [],
    "description": "string",
    "email_message": "string",
    "email_subject": "string",
    "enabled": true,
    "from": "string",
    "id": 0,
    "include_links": "string",
    "name": "string",
    "output": {},
    "owner": "string",
```

```
    "schedule": {},
    "until": "string"
}
```

`GET /reports/{id}/download`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the report.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "cc": [],
    "description": "string",
    "email_message": "string",
    "email_subject": "string",
    "enabled": true,
    "from": "string",
    "id": 0,
    "include_links": "string",
    "name": "string",
    "output": {},
    "owner": "string",
    "schedule": {},
    "until": "string"
}
```

`DELETE /reports/{id}`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the report.

`GET /reports/{id}/contents`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the report.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "dashboard_id": 0,
    "params": {},
    "type": "string"
}
```

`PUT /reports/{id}/contents`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the report.

`body:` ***Object***
The contents of the report.

Software

You can view a list of software that the ExtraHop system has observed on your network.

Operation	Description
GET /software	Retrieve software observed by the ExtraHop system.
GET /software/{id}	Retrieve software observed by the ExtraHop system by ID.

Operation details

`GET /software`

Specify the following parameters.

`software_type:` ***String***
(Optional) The type of software.

`name:` ***String***
(Optional) The name of the software.

`version:` ***String***
(Optional) The version of the software.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "description": "string",
    "id": "string",
    "name": "string",
    "software_type": "string",
    "version": "string"
}
```

`GET /software/{id}`

Specify the following parameters.

`id:` ***String***
The unique identifier for the software.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "description": "string",
    "id": "string",
    "name": "string",
    "software_type": "string",
    "version": "string"
}
```

Tag

Device tags enable you to associate a device or group of devices by some characteristic.

For example, you might tag all of your HTTP servers or tag all of the devices that are in a common subnet. For more information, see Tag a device through the REST API.

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /tags	Retrieve all tags.
POST /tags	Create a a new tag.
DELETE /tags/{id}	Delete a specific tag.
GET /tags/{id}	Retrieve a specific tag.
PATCH /tags/{id}	Apply updates to a specific tag.
GET /tags/{id}/devices	Retrieve all devices that are assigned to a specific tag.
POST /tags/{id}/devices	Assign and unassign a specific tag to devices.
DELETE /tags/{id}/devices/{child-id}	Unassign a device from a specific tag.
POST /tags/{id}/devices/{child-id}	Assign a device to a specific tag.

Operation details

`GET /tags`

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "id": 0,
    "mod_time": 0,
    "name": "string"
}
```

`POST /tags`

Specify the following parameters.

`body:` ***Object***

Apply the specified property values to the new tag.

`name:` ***String***

The string value for the tag.

Specify the body parameter in the following JSON format.

```
{
    "name": "string"
}
```

`GET /tags/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the tag.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "id": 0,
    "mod_time": 0,
    "name": "string"
}
```

`DELETE /tags/{id}`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the tag.

`PATCH /tags/{id}`

Specify the following parameters.

`body:` ***Object***
Apply the specified property value updates to the tag.
`id:` ***Number***
The unique identifier for the tag.

`GET /tags/{id}/devices`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the tag.

`POST /tags/{id}/devices`

Specify the following parameters.

`body:` ***Object***
Lists of unique identifies for device to assign and unassign.
`assign:` ***Array of Numbers***
IDs of resources to assign
`unassign:` ***Array of Numbers***
IDs of resources to unassign
Specify the body parameter in the following JSON format.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Number***
The unique identifier for the tag.

`POST /tags/{id}/devices/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the device.
`id:` ***Number***
the unique identifier for the tag.

```
DELETE /tags/{id}/devices/{child-id}
```

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the device.
`id:` ***Number***
The unique identifier for the tag.

Threat Collection

The Threat Collection resource enables you to upload free and commercial threat collections offered by the security community to your Reveal(x) system.

- You must upload threat collections individually to your Command appliance or Reveal(x) 360, and to all connected sensors.
- Custom threat collections must be formatted in Structured Threat Information eXpression (STIX) as TAR.GZ files. Reveal(x) currently supports STIX version 1.0 - 1.2.
- You can directly upload threat collections to Reveal(x) 360 systems for self-managed sensors. Contact ExtraHop Support to upload a threat collection to ExtraHop-managed sensors.
- The maximum number of observables that a threat collection can contain depends on your platform and license. Contact your ExtraHop representative for more information.

Note: This topic applies only to ExtraHop Reveal(x) Premium and Ultra.

For information about uploading STIX files through the ExtraHop system, see Upload STIX files through the REST API.

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /threatcollections	Retrieve all threat collections.
POST /threatcollections	Create a new threat collection.
DELETE /threatcollections/{id}	Delete a threat collection.
PUT /threatcollections/{id}	Upload a new threat collection. ExtraHop currently supports STIX versions 1.0 - 1.2. **Note:** If a threat collection with the same name already exists on the ExtraHop system, the existing threat collection is overwritten.
GET /threatcollections/{id}/observables	Retrieve the number of STIX observables loaded from a threat collection, such as IP address, hostname, or URI.

Operation details

`GET /threatcollections`

There are no parameters for this operation.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "id": 0,
    "last_updated": 0,
    "name": "string",
    "observables": 0,
    "user_key": "string"
}
```

`POST /threatcollections`

Specify the following parameters.

`user_key:` ***String***
(Optional) The user-supplied identifier for the threat collection. If this parameter is not specified, the threat collection name is set for this value, without spaces or punctuation.

`name:` ***String***
The name for the threat collection.

`file:` ***Filename***
The filename for the threat collection.

`PUT /threatcollections/~{userKey}`

Specify the following parameters.

`userKey:` ***String***
The user-supplied identifier for the threat collection.

`name:` ***String***
(Optional) The name for the threat collection.

`file:` ***Filename***
(Optional) The filename for the threat collection.

`DELETE /threatcollections/{id}`

Specify the following parameters.

`id:` ***String***
The unique identifier for the threat collection.

`GET /threatcollections/{id}/observables`

Specify the following parameters.

`id:` ***String***
The unique identifier for the threat collection.

Trigger

Triggers are custom scripts that perform an action upon a pre-defined event.

For example, you can write a trigger to record a custom metric every time an HTTP request occurs, or classify traffic for a particular server as an Application server. For more information, see the Trigger API Reference. For supplemental implementation notes about advanced options, see Advanced trigger options.

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /triggers	Retrieve all triggers.
POST /triggers	Create a new trigger.
POST /triggers/externaldata	Sends data to the Trigger API by running the EXTERNAL_DATA event. You can access the data through the ExternalData trigger class. **Note:** This operation is not available for Command appliances or Reveal(x) 360.
DELETE /triggers/{id}	Delete a specific identifier.
GET /triggers/{id}	Retrieve a specific trigger by unique identifier.
PATCH /triggers/{id}	Update an existing trigger.
GET /triggers/{id}/devicegroups	Retrieve all device groups that are assigned to a specific trigger.
POST /triggers/{id}/devicegroups	Assign and unassign a specific trigger to device groups.
DELETE /triggers/{id}/devicegroups/{child-id}	Unassign a device group from a specific trigger.
POST /triggers/{id}/devicegroups/{child-id}	Assign a device group to a specific trigger.
GET /triggers/{id}/devices	Retrieve all devices that are assigned to a specific trigger.
POST /triggers/{id}/devices	Assign and unassign a specific trigger to devices.
DELETE /triggers/{id}/devices/{child-id}	Unassign a device from a specific trigger.
POST /triggers/{id}/devices/{child-id}	Assign a device to a specific trigger.

Operation details

`GET /triggers`

There are no parameters for this operation.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "apply_all": true,
    "author": "string",
    "debug": true,
    "description": "string",
    "disabled": true,
    "event": "string",
```

```
    "events": [
        "string"
    ],
    "hints": {},
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "script": "string"
}
```

`DELETE /triggers/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the trigger.

`POST /triggers/externaldata`

Specify the following parameters.

`body:` ***Object***

The object containing the data to send to triggers through the EXTERNAL_DATA event.

`type:` ***String***

A string identifier that describes the data contained in the body parameter. For example, you could specify 'phantom-data' for data sent from the Phantom SOAR platform.

`body:` ***Object***

The data to send to triggers through the EXTERNAL_DATA event. This data can be accessed in the trigger with the 'ExternalData.body' property.

Specify the body parameter in the following JSON format.

```
{
    "body": {},
    "type": "string"
}
```

`POST /triggers`

Specify the following parameters.

`body:` ***Object***

The property values for the new trigger.

`name:` ***String***

The friendly name for the trigger.

`description:` ***String***

(Optional) An optional description of the trigger.

`author:` ***String***

The name of the creator of the trigger.

`script:` ***String***

The JavaScript content of the trigger.

`event:` ***String***

(Optional) Deprecated. Replaced by the events field.

`events:` ***Array of Strings***

The list of events on which the trigger runs, expressed as a JSON array.

`disabled:` ***Boolean***

Indicates whether the trigger can run.

`debug:` ***Boolean***

Indicates whether debug statements are printed for the trigger.

`apply_all:` ***Boolean***

Indicates whether the trigger applies to all relevant resources.

`hints:` ***Object***

Options that are based on selected trigger events. For more information about the hints object, see the REST API Guide.

Specify the body parameter in the following JSON format.

```
{
    "apply_all": true,
    "author": "string",
    "debug": true,
    "description": "string",
    "disabled": true,
    "event": "string",
    "events": [
        "string"
    ],
    "hints": {},
    "name": "string",
    "script": "string"
}
```

`PATCH /triggers/{id}`

Specify the following parameters.

`body:` ***Object***

The property value updates for the trigger.

`id:` ***Number***

The unique identifier for the trigger.

`GET /triggers/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the trigger.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "apply_all": true,
    "author": "string",
    "debug": true,
    "description": "string",
    "disabled": true,
    "event": "string",
    "events": [
        "string"
    ],
```

```
    "hints": {},
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "script": "string"
}
```

`GET /triggers/{id}/devicegroups`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the trigger.

`POST /triggers/{id}/devicegroups`

Specify the following parameters.

`body:` ***Object***
A list of unique identifiers for device groups that are assigned and unassigned to a trigger.
`assign:` ***Array of Numbers***
IDs of resources to assign
`unassign:` ***Array of Numbers***
IDs of resources to unassign
Specify the body parameter in the following JSON format.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Number***
The unique identifier for the trigger.

`POST /triggers/{id}/devicegroups/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the device group.
`id:` ***Number***
The unique identifier for the trigger.

`DELETE /triggers/{id}/devicegroups/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the device group.
`id:` ***Number***
The unique identifier for the trigger.

`GET /triggers/{id}/devices`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the trigger.

`POST /triggers/{id}/devices`

Specify the following parameters.

`body:` ***Object***
A list of unique identifiers for devices that are assigned and unassigned to a trigger.
`assign:` ***Array of Numbers***
IDs of resources to assign
`unassign:` ***Array of Numbers***
IDs of resources to unassign

Specify the body parameter in the following JSON format.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Number***
The unique identifier for the trigger.

`POST /triggers/{id}/devices/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the device.
`id:` ***Number***
The unique identifier for the trigger.

`DELETE /triggers/{id}/devices/{child-id}`

Specify the following parameters.

`child-id:` ***Number***
The unique identifier for the device.
`id:` ***Number***
The unique identifier for the trigger.

User group

The user group resource enables you to manage and update groups of users and their dashboard sharing associations.

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /usergroups	Retrieve all user groups.
POST /usergroups	Create a new user group.
DELETE /usergroups/{id}	Delete a specific user group.

Operation	Description
GET /usergroups/{id}	Retrieve a specific user group.
PATCH /usergroups/{id}	Update a specific user group.
DELETE /usergroups/{id}/associations	Delete all dashboard sharing associations with a specific user group.
GET /usergroups/{id}/members	Retrieve all members of a specific user group.
PATCH /usergroups/{id}/members	Assign or unassign users from a user group.
PUT /usergroups/{id}/members	Replace user group assignments.

Operation details

`GET /usergroups`

There are no parameters for this operation.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "display_name": "string",
    "enabled": true,
    "id": "string",
    "is_remote": true,
    "last_sync_time": 0,
    "name": "string",
    "rights": []
}
```

`POST /usergroups`

Specify the following parameters.

`body:` ***Object***

The properties of the user group.

`name:` ***String***

The name for the user group.

`enabled:` ***Boolean***

Indicates whether the user group is enabled.

Specify the body parameter in the following JSON format.

```
{
    "enabled": true,
    "name": "string"
}
```

`PATCH /usergroups/{id}`

Specify the following parameters.

`body:` ***Object***

The property value updates for the specific user group.

`id:` ***String***
The unique identifier for the user group.

`GET /usergroups/{id}`

Specify the following parameters.

`id:` ***String***
The unique identifier for the user group.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "display_name": "string",
    "enabled": true,
    "id": "string",
    "is_remote": true,
    "last_sync_time": 0,
    "name": "string",
    "rights": []
}
```

`DELETE /usergroups/{id}`

Specify the following parameters.

`id:` ***String***
The unique identifier for the user group.

`DELETE /usergroups/{id}/associations`

Specify the following parameters.

`id:` ***String***
The unique identifier for the user group.

`GET /usergroups/{id}/members`

Specify the following parameters.

`id:` ***String***
The unique identifier for the user group.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "users": {}
}
```

`PATCH /usergroups/{id}/members`

Specify the following parameters.

`id:` ***String***
The unique identifier for the user group.

`body:` ***String***

An object that specifies which users to asssign or unassign. Each key must be a username and each value must be either "member" or null. For example {"Alice": "member", "Bob": null} assigns Alice to the group and unassigns Bob from the group.

`PUT /usergroups/{id}/members`

Specify the following parameters.

`id:` ***String***

The unique identifier for the user group.

`body:` ***String***

An object that specifies which users are assigned to the group. Each key must be a username and each value must be "member". For example {"Alice": "member", "Bob": "member"} assigns Alice and Bob as the only members of the group.

VLAN

Virtual LANs are logical groupings of traffic or devices on the network.

The following table displays all of the operations you can perform on this resource:

Operation	Description
GET /vlans	Retrieve all VLANs
GET /vlans/{id}	Retrieve a specific VLAN.
PATCH /vlans/{id}	Update a specific VLAN.

Operation details

`GET /vlans`

There are no parameters for this operation.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
    "description": "string",
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "network_id": 0,
    "node_id": 0,
    "vlanid": 0
}
```

`GET /vlans/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the VLAN.

If the request is successful, the ExtraHop system returns an object in the following format.

```
{
```

```
    "description": "string",
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "network_id": 0,
    "node_id": 0,
    "vlanid": 0
}
```

`PATCH /vlans/{id}`

Specify the following parameters.

`body:` ***Object***

Apply the specified property value updates to the VLAN.

`id:` ***Number***

The unique identifier for the VLAN.

Watchlist

To guarantee that an asset, such as an important server, database, or laptop, is guaranteed Advanced Analysis, you can add that device to the watchlist.

Tip: If you want to add several devices to the watchlist, consider creating a device group and then prioritizing that group for Advanced Analysis.

Here are important considerations about the watchlist:

- The watchlist only applies to Advanced Analysis.
- The watchlist can contain as many devices as allowed by the Advanced Analysis capacity, which is determined by your license.
- A device stays on the watchlist whether it is inactive or active. A device has to be active for the ExtraHop system to collect Advanced Analysis metrics.

For more information about Advanced Analysis, see Analysis levels.

The following table displays all of the operations you can perform on this resource:

Operation	Description
DELETE /watchlist/device/{id}	Remove a device from the watchlist.
POST /watchlist/device/{id}	Add a device to the watchlist.
GET /watchlist/devices	Retrieve all devices that are in the watchlist.
POST /watchlist/devices	Add or remove devices from the watchlist.

Operation details

`GET /watchlist/devices`

There are no parameters for this operation.

`POST /watchlist/device/{id}`

Specify the following parameters.

`id:` ***Number***

The unique identifier for the device.

`DELETE /watchlist/device/{id}`

Specify the following parameters.

`id:` ***Number***
The unique identifier for the device.

`POST /watchlist/devices`

Specify the following parameters.

`assignments:` ***Object***
A list of devices to add to or remove from the watchlist.

`assign:` ***Array of Numbers***
IDs of resources to assign

`unassign:` ***Array of Numbers***
IDs of resources to unassign

Specify the assignments parameter in the following JSON format.

```
{
    "assign": [],
    "unassign": []
}
```